televic
Providers of reliable interaction

Confidea ©

Wireless Conference System

Installation and User Manual

Table of Contents

Table of Contents **2**

Section 1 – General Information **7**

1. Copyright Statement **9**

2. Trademarks **10**

3. Safety Instructions and conformity info **11**

3.1. FCC and ICES information **11**
3.1.1. Statements for FCC and Industry Canada 11

3.2. Conformity and Certification info for Japan **12**
3.3. Important safety instructions **12**
3.4. General conformity info **14**
3.5. Power Connections **15**

4. Confidea wireless System Information **16**

4.1. General System Architecture **16**
4.1.1. Components 16
4.1.2. Stand-alone system 16
4.1.3. Connected to Televic wired conference system 16

5. Wireless networks and frequency bands **17**

5.1. Wireless LAN **17**
5.2. Televic Confidea wireless system **17**
5.2.1. Frequency bands 17

5.3. Frequency Planning **18**
5.3.1. Use with WiFi base stations nearby 18
5.3.2. Use of multiple Confidea wireless systems 19

5.4. Max range of WCAP **19**
5.5. Guidelines on optimal WCAP positioning and direction of antennas **20**
5.5.1. Positioning the Confidea Wireless Access Point 20
5.5.2. Optimizing the position the antennas 20

Section 2 – System Components **22**

6. Wireless contribution units 23

6.1. Introduction 23
6.2. Controls and indicators 23
6.3. Installation 32
6.4. Maintenance 32
6.4.1. General 32
6.4.2. Cleaning 32

6.5. Startup and shutdown 33

7. Microphones 33
7.1. Introduction 33
7.2. Electrical and acoustic properties 33
7.3. Microphone connector 34
7.4. Operation 34
7.5. Installation and handling 35

8. Battery Pack 36

8.1. Introduction 36
8.2. Safety 36
8.3. Controls and indicators 37
8.4. Installation 37
8.5. Storage and discharge behaviour 38
8.5.1Store at low temperature 38
8.5.2Store at 50% charge 38
8.5.3Remove from unit for long term storage 38

9. Wall plug battery charger 39

9.1. Introduction 39
9.2. Installation 39
9.3. Charging a battery pack 40
9.4. Use of battery charging tray 41

10. Wireless Conference Access Point (WCAP) 42

10.1. Introduction 42
10.2. Installation 42
10.2.1. General 42
10.2.2. Wall Mounting 42
10.2.3. Tripod Mounting 42
10.2.4. Antennas 42

10.3. Connections and Controls 43

Section 3 – System Configuration 45

11. Accessing the built-in web server 47

11.1. Introduction 47
11.2. First time access 47
11.2.1. Step 1 – Reset 47
11.2.2. Step 2 – PC or MAC TCP/IP setup 48
11.2.3. Step 3 – Cable Setup 53
11.2.4. Step 4 – Accessing WCAP 53
11.2.5. Step 5 – Default Screen 54

11.3. Setting the IP address 54
11.4. Updating SW 55

12. Web server 59

12.1. Setup 59
12.1.1. Summary 59
12.1.2. TCP/IP settings 60
12.1.3. Country selection 60
12.1.4. Admin 60
12.1.5. License 61

12.2. RF Configuration 61
12.2.1. General 61
12.2.2. Quality 2.4 GHz ISM 62
12.2.3. Quality 5.15 – 5.35 GHz 62
12.2.4. Quality 5.47 – 5.725 GHz 62
12.2.5. Quality 5.8 GHz ISM 62

12.3. Conference Management 63
12.3.1. General 63
12.3.2. Unit Monitoring 66
12.3.3. Init Units 66

12.4. Service 67
12.4.1. Logging 67

12.5. Encryption 67
12.5.1. Key Assignment 67

13. Initialization 69

13.1. Introduction 69

13.2. Stand-alone mode 69
13.2.1. Access modes 69
13.2.2. Selecting the Access Mode 69
13.2.3. Unit initialization in 'Open Access' mode 70
13.2.4. Unit initialization in 'Controlled Access' mode 70
13.2.5. Adding a new unit in 'Open Access' mode 71
13.2.6. Adding a new unit in 'Controlled Access' mode 71
13.2.7. Reviewing Init information 72

13.3. Coupled mode 72

14. Using Encryption 73

14.1. Introduction 73
14.2. Default encryption 73
14.3. Setting the default encryption 73
14.4. Custom encryption 74
14.5. Setting a customized encryption 74
14.6. Adding a unit with a customized encryption 76
14.7. Using multiple customized keys 76

15. Auxiliary in/out 77

15.1. Introduction 77
15.2. Use of Auxiliary input - output 77
15.2.1. Distance conferencing 77
15.2.2. External Processing 77

15.3. Selecting auxiliary input/output settings 77
15.4. Signal paths 78
15.4.1. Stand alone mode 78
15.4.2. External processing 78
15.4.3. N-1 or Distance Conferencing 78

15.5. Aux signal levels 78

Section 4 – Use Cases 79

16. Stand alone system 81

16.1. Basic discussion 81
16.2. Basic voting and opinion polling 82

17. Connected to CE2500, Confidea CU or CPU5500 84

17.1. Discussion 86

17.2. Advanced Voting 88
17.3. Interpretation 88

Section 5 – Appendix 91

18. Default Settings 93

18.1. TCP/IP settings 93
18.1.1. Identification 93
18.1.2. IP Configuration 93

18.2. Country Selection 93
18.3. Admin 93
18.4. RF Configuration 93
18.4.1. Power 93
18.4.2. Frequency 93

18.5. Conference Management 93
18.5.1. Conference Configuration 93
18.5.2. Interpreter Configuration 93
18.5.3. Operating Mode 93

18.6. Init Control 93
18.7. Encryption 93

Section 1 – General Information

1. Copyright Statement

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without the prior written permission of the publisher, except in case of brief quotations embodied in critical articles or reviews. Contents are subject to change without prior notice.

Copyright© 2008 by Televic NV. All rights reserved.

The authors of this manual have made every effort in the preparation of this book to ensure the accuracy of the information. However, the information in this manual is supplied without warranty, either express or implied. Neither the authors, Televic NV, nor its dealers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

2. Trademarks

All terms mentioned in this manual that are known to be trademarks or service marks have been appropriately capitalized. Televic NV cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

3. Safety Instructions and conformity info

The Confidea Wireless Conference system is state of the art and has been designed to meet quality. Nevertheless, the individual components of the conference system can cause danger for persons and material assets if

- the conference system is not used as intended,
- the conference system is set up by personnel not familiar with the safety regulations,
- the conference system is converted or altered incorrectly,
- the safety instructions are not observed.

3.1. FCC and ICES information

(U.S.A and Canadian Models only)

3.1.1. Statements for FCC and Industry Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The Confidea wireless equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Wireless discussion units and the Wireless Access Point comply with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Warning:
Changes or modifications made to this equipment not expressly approved by Televic NV may void the FCC authorization to operate this equipment.

Radiofrequency radiation exposure Information:
This Wireless discussion units and the Wireless Access Point comply with FCC radiation exposure limits set forth for an uncontrolled environment. These Wireless discussion units and the Wireless Access Point should be installed and operated with minimum distance of 20 cm between the radiator and your body.

The RF-parts of the Wireless discussion units and the Wireless Access Point must not be co-located or operating in conjunction with any other antenna or transmitter.

3.2. Conformity and Certification info for Japan

This device has been granted a designation number by Ministry of In-ternal Affairs andCommunications: according:
Ordinance concerning Technical Regulations Conformity Certification etc. of Specified Radio Equipment (特定無線設備の技術基準適合証明等に関する規則)

Article 2 clause 1 item 19/3

Approval n°: 202WW10120791/2"
202XW10120791/2

Warning:
This device should not be modified, otherwise the granted designation number will be invalid.

3.3. Important safety instructions

1. Read Instructions

All the safety and operating instructions should be read before the product is operated.

2. Retain Instructions

The safety and operating instructions should be retained for future reference.

3. Heed Warnings

All warnings on the product and the operating instructions should be adhered to.

4. Follow Instructions

All instructions for installation or operating / use should be followed.

5. Cleaning

Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.

6. Ventilation

Slots and openings in the cabinet are provided for ventilation and to ensure reliable operation of the product and to protect it from overheating. These openings must not be blocked or covered. The openings should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should not be placed in a built-in installation such as a bookcase or rack unless proper ventilation is provided or the manufacturer's instructions have been adhered to.

7. Heat

The product should be situated away from heat sources such as radiators, heat registers, stoves, or other products (including amplifiers) that produce heat.

8. Attachments

Do not use attachments not recommended by the product manufacturer as they may cause hazards.

9. Water and Moisture

Do not use this product near water or in a moistures environment - for example, near a bath tub, wash bowl, kitchen sink, or laundry tub; in a wet basement; or near a swimming pool, in an unprotected outdoor installation; and the like.

10. Accessories

Only use attachments/accessories specified by the manufacturer. Do not place this product on an unstable cart, stand, tripod, bracket, or table. The product may fall, causing serious injury to a child or adult, and serious damage to the product. Use only with a cart, stand, tripod, bracket, or table recommended by the manufacturer, or sold with the product. Any mounting of the product should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.

11. Moving

A product and cart combination should be moved with care. Quick stops, excessive force, and uneven surfaces may cause the product and cart combination to overturn.

12. Power Sources

This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply to your home, consult your product dealer or local power company. For products intended to operate from battery power, or other sources, refer to the operating instructions.

13. Power Lines

An outdoor system should not be located in the vicinity of overhead power lines or other electric light or power circuits, or where it can fall into such power lines or circuits. When installing an outdoor system, extreme care should be taken to keep from touching such power lines or circuits, as contact with them might be fatal. U.S.A. models only - refer to the National Electrical Code Article 820 regarding installation of CATV systems.

14. Grounding or Polarization

Do not defeat the safety purpose of the polarized or ground-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wider blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.

15. Power-Cord Protection

Power-supply cords should be routed to that they are not likely to be walked on or pinched by items placed upon or against them, paying particular attention to cords at plug, convenience receptacles, and the point where they exit from the product.

16. Lightning

For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet. This will prevent damage to the product due to lightning and power-line surges.

Not applicable when special functions are to be maintained, such as evacuation systems

17. Overloading

Do not overload wall outlets, extension cords or integral convenience receptacles as this can result in a risk of fire or electric shock.

18. Object and Liquid Entry

Never push objects of any kind into this product through openings as they may touch dangerous voltage points or short-out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.

19. Inflammable and Explosive Substance

Avoid using this product where there are gases, and also where there are inflammable and explosive substances in the immediate vicinity.

20. Heavy Shock or Vibration

When carrying this product around, do not subject the product to heavy shock or vibration.

21. Servicing

Do not attempt to service this product yourself as opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.

22. Damage Requiring Service

Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

a. When the power-supply cord or plug is damaged.

b. if liquid has been spilled, or objects have fallen into the product.

c. If the product has been exposed to rain or water.

d. If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions as an improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to its normal operation.

e. If the product has been dropped or damaged in any way.

f. When the product exhibits a distinct change in performance-this indicates a need for service.

23. Replacement Parts

When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock, or other hazards.

24. Safety Check

Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in proper operating condition.

25. Coax Grounding

If an outside cable system is connected to the apparatus, be sure the cable system is grounded. U.S.A. models only: Section 810 of the National Electrical Code, ANSI/NFPA No.70-1981, provides information with respect to proper grounding of the mount and supporting structure, grounding of the coax to a discharge apparatus, size of grounding conductors, location of discharge unit, connection to grounding electrodes, and requirements for the grounding electrode.

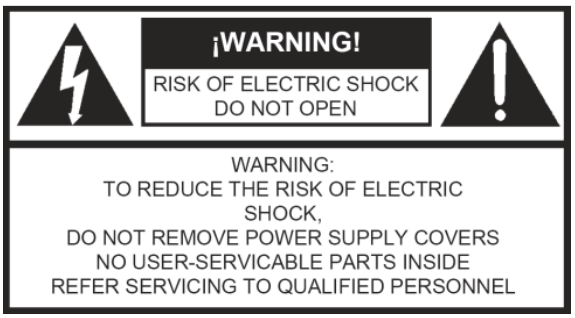
3.4. General conformity info

The Confidea Wireless Conference system is compliant with following standards:

- EN60065
- EN55103-1/-2
- IEC60914

3.5. Power Connections

For permanently connected equipment, a readily accessible disconnect device shall be incorporated in the fixed wiring; For pluggable equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.



This label may appear on the bottom of the apparatus due to space limitations.

The lightning flash with an arrowhead symbol, with an equilateral triangle, is intended to alert the user to the presence of un-insulated 'dangerous voltage' within the products enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

The exclamation mark within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Warning:
To reduce the risk of fire or electric shock, do not expose this appliance to rain or moisture. Do not open the cabinet; refer servicing to qualified personnel only.

Warning:
To prevent electric shock, do not use this (polarized) plug with an extension cord receptacle or other outlet unless the blades can be fully inserted to prevent blade exposure.

Attention:
Installation should be performed by qualified service personnel only in accordance with the National Electrical Code or applicable local codes.

Attention:
Equipment with or without ON/OFF switches have power supplied to the equipment whenever the power cord is inserted into the power source; however, the equipment is operational only when the ON/OFF switch is in the ON position. The power cord is the main power disconnect for all equipment.

4. Confidea wireless System Information

4.1. General System Architecture

4.1.1. Components

Confidea wireless is a wireless conference system offering conferencing facilities over a robust wireless link. Depending on the model, these facilities include discussion, voting and/or language distribution.

The delegate units are stand-alone, table top units that connect in a wireless manner to the Confidea Wireless Conference Access Point (WCAP). This Access Point has a built-in web server that allows configuring and monitoring of the system from any PC or laptop with a network card, using a standard internet browser.

Depending on the application, Confidea wireless can be configured as a standalone system, but can also be integrated into an existing Televic Confidea CU or TCS5500 system.

Note:

Confidea wireless webserver has been fully tested successfully on Windows Internet Explorer 8.

However , since there exists a wide variaty of web browsers , which are subject to regular updates , 100% correct functionality of Confidea wireless webserver on all browser types can not be guaranteed, because some actions may be blocked by specific browsers.

4.1.2. Stand-alone system

A stand-alone Confidea wireless system offers basic discussion and basic voting or opinion polling (depending on the model).

In this case there are no connections to other systems, except for the Confidea WCAP that can be connected to a LAN network for monitoring and configuring.

The Confidea access point (WCAP) will in this set-up act as a small central unit, offering all the functionality for a basic discussion and/or opinion polling application.

4.1.3. Connected to Televic wired conference system

As part of a wired system, the Confidea wireless offers full functionality such as extended voting facilities and language distribution. When connected to a Confidea CU or TCS5500 central unit, the Confidea wireless delegates become an integral part of the wired system.

5. Wireless networks and frequency bands

5.1. Wireless LAN

Most of the wireless local area computer networks today are based on the IEEE 802.11 a/b/g standards. These standards were developed by the IEEE (Institute of Electrical and Electronics Engineers) in order to insure inter-operability between different WLAN vendors. Refer to Table 5.1: Wireless LAN standardsTable 5.1 for an overview of the different standards:

Table 5.1: Wireless LAN standards

802.11 Standard	Release Date	Frequency (GHz)	Maximum bit rate (Mbits/sec)	Modulation type
a	1999	5	54	OFDM
b	1999	2.4	11	DSSS
g	2003	2.4	54	OFDM

Note:
The 2.4GHz and 5GHz frequency bands are license free world wide.
However you must be aware of country specific limitations and follow them.

5.2. Televic Confidea wireless system

The wireless network of the Televic Confidea wireless system is based on the 802.11 a/g standards.

Additional protocols have been added on top of the 802.11 a/g standards to provide high robustness against interference from other wireless devices. These additional protocols also ensure a guaranteed quality of service for the audio streams on the wireless network.

5.2.1. Frequency bands

The Confidea wireless system supports the following frequency bands (refer to Table 5.2):

Table 5.2: Frequency bands supported by Confidea

ISM 2.4 GHz	RLAN low	RLAN high	ISM 5 GHz
2412 MHz	5180 MHz	5500 MHz	5745 MHz
2417 MHz	5200 MHz	5520 MHz	5765 MHz
2422 MHz	5220 MHz	5540 MHz	5785 MHz
2427 MHz	5240 MHz	5560 MHz	5805 MHz
2432 MHz	5260 MHz	5580 MHz	
2437 MHz	5280 MHz	5600 MHz	
2442 MHz	5300 MHz	5640 MHz	
2447 MHz	5320 MHz	5660 MHz	
2452 MHz		5680 MHz	
2457 MHz		5700 MHz	
2462 MHz			
2467MHz			
2472 MHz			

In the **2.4 GHz ISM** (Industrial Scientific Medical) band, there are 13 overlapping high-frequency carriers available. Only 3 non-overlapping carriers are available.

Allowed 2.4 GHz ISM band carriers In Europe :
all 13 carriers of 2.4 GHz ISM band may be used.

Allowed 2.4 GHz ISM band carriers In the USA and Canada (FCC regulations) ;
the 2 highest wireless carriers of the 2.4 GHz ISM band , may not be be used
(CH12 - 2467 MHz and CH13 - 2472 MHz).

Allowed 2.4GHz ISM band carriers in Japan;
the 2 highest wireless carriers of the 2.4 GHz ISM band , may not be be used
(CH12 - 2467 MHz and CH13 - 2472 MHz).

In the "**RLAN low**" frequency band, there are 8 non-overlapping wireless carriers

Allowed RLAN low band carriers in Europe;
all 8 carriers may be used

Allowed RLAN low band carriers in USA and Canada (FCC regulations) ;
only the 4 lowest wireless carriers may be used (5180 MHz – 5200 MHz – 5220MHz – 5240MHz).

Allowed RLAN low band carriers in Japan ;
only the 4 lowest wireless carriers may be used (5180 MHz – 5200 MHz – 5220MHz – 5240MHz).

In the "**RLAN high**" frequency band, there are 10 non-overlapping carriers.

Allowed RLAN high band carriers in Europe;
All these carriers may be used

Allowed RLAN high band carriers in USA and Canada (FCC regulations) ;
these carriers may not be used.

Allowed RLAN high band carriers in Japan;
these carriers may not be used.

In the "**5 GHz ISM"** frequency band, there are 4 non-overlapping carriers. All of these carriers can be used.

Allowed 5 GHz ISM band carriers in Europe;
All these carriers may be used

Allowed 5 GHz ISM band carriers in USA and Canada (FCC regulations) ;
All these carriers may be used.

Allowed 5 GHz ISM band carriers in Japan;
All these carriers may be used.

Note:
The user can choose to set the wireless carriers manually or let the CONFIDEA system automatically select the best wireless carrier frequency.

5.3. Frequency Planning

5.3.1. Use with WiFi base stations nearby

When the Confidea wireless system is set to automatically select the carrier frequency, the Confidea wireless carrier frequency will be dynamically switched to another channel if an existing WiFi device occupies the same channel. This dynamic frequency allocation ensures high robustness of the system even if the frequency occupation changes during the meeting.

When the Confidea wireless system is set to manually select the wireless carrier frequency, then you must make sure the Confidea wireless carrier does not overlap the already occupied WiFi wireless carrier channels.

Note :

Wifi access points and use of 5gHz band

Some wifi accesspoints which support IEEE 802.11n may also use 5gHz band when they are configured in DualBand or Backhaul mode!

5.3.2. Use of multiple Confidea wireless systems

When the Confidea wireless system is set to automatically select the carrier frequency, the Confidea carrier frequency will be dynamically set to another channel if another Confidea wireless system occupies the same channel. This dynamic frequency allocation ensures that each Confidea wireless system will be set automatically to different frequencies.

When the Confidea wireless system is set to manually select the wireless carrier frequency, you must make sure the Confidea wireless carriers of the different rooms do not overlap each other.

Note :

Manual or automatic frequency selection?

If more than one WCAP or Wifi accesspoints are in the same room or within 30m. range , it is strongly advised that not more than one of them uses automatic frequency selection , to avoid that the frequencyscanning is disturbed by the other accesspoint(s) . If multiple accesspoints are used within each other's reach, manual frequency selection based on frequency planning is strongly recommended .

Note :

Selecting frequency

When using manual frequency selection in 5gHz band , ideally the frequency selection is done in such way that between 2 used frequencies , there is a 40Mhz "distance" to avoid interference by RF sidebands.

5.4. Max range of WCAP

A single WCAP has a range of 30m in "open field" . However the max range can be significantly less depending on the positioning of the WCAP itself and direction of the antennas in relation to the position of the delegate units.

See chapter 5.5 for detailed info

Attention:

Certain buildingmaterials like concrete , or metal may absorb part of the RF signalradiation, resulting in a reduction of the max distance between the access point and units.

5.5. Guidelines on optimal WCAP positioning and direction of antennas

Attention:
Do not place the WCAP behind obstacles like walls , cabinets, panels, projection screen, glass screens etc… , as they significantly reduce RF signal strength and quality

5.5.1. Positioning the Confidea Wireless Access Point

Below you can find how to select a correct positioning of the WCAP.

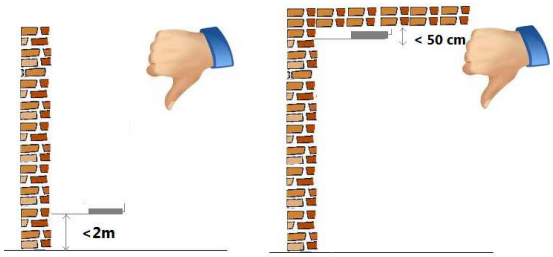


Figure 5.1 WCAP position hight

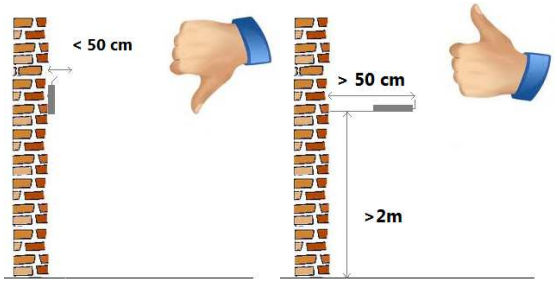


Figure 5.2 WCAP position to wall

Note :

When the antennas of the WCAP are positioned very close to a wall or ceiling , this may result in absorption of the RF signal , which can decrease RF signal quality.

5.5.2. Optimizing the position the antennas

Note :

It is important **not** to point the antennas directly to the units

Figure 5.3 WCAP position antennas

for detailed view see of optimal antenna positioning see Figure 5.4 WCAP position antennas

Note :

Choosing the correct angle of the antennas in relation to the position of the delegate units is beneficial to a good overall RF link quality between WCAP and delegate units

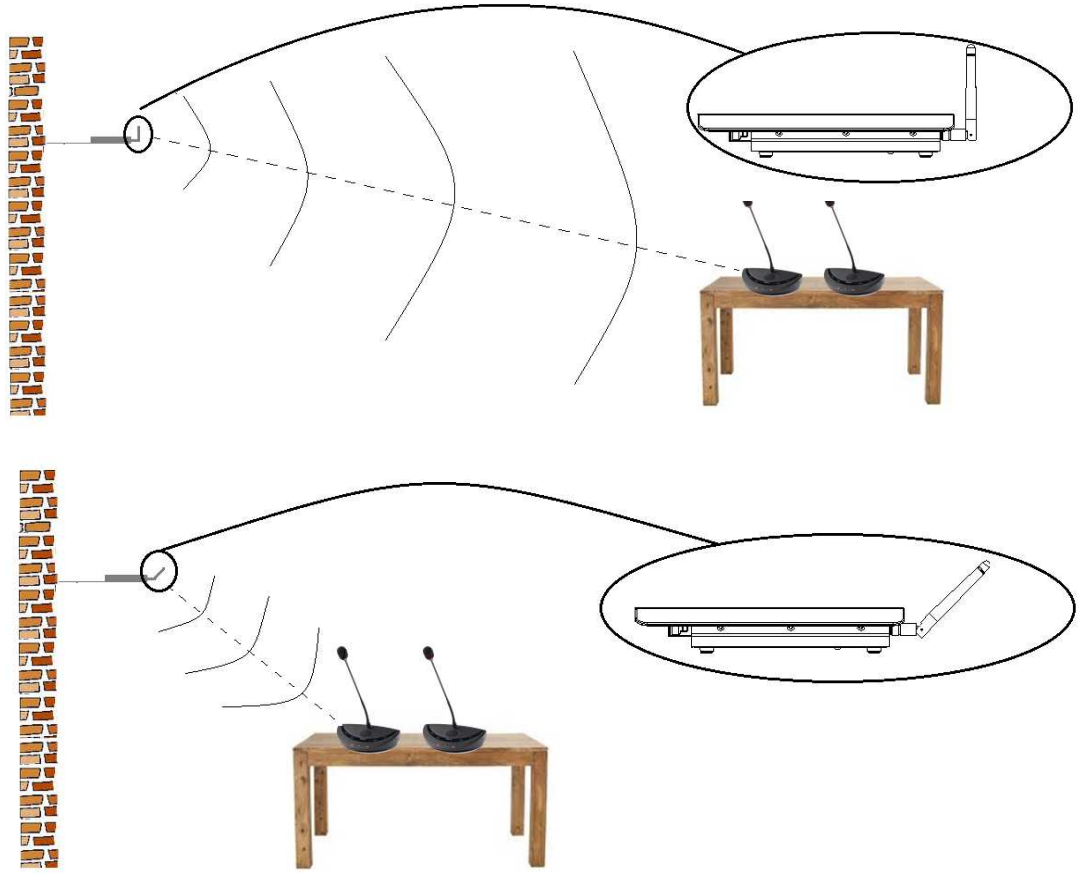


Figure 5.4 WCAP position antennas

Section 2 – System Components

6. Wireless contribution units

6.1. Introduction

The wireless contribution units , called *Confidea WDU* , consist of Delegate and Chairman units. Both are used for speech reinforcement in a conference room. The chairman units are used to guide and control an ongoing discussion.

The units can be divided into three categories:

- Discussion :
  Confidea DD (Figure 6.1), CD(Figure 6.2), 2D2D (Figure 6.3: Confidea 2D2D)
- Voting :
  Confidea DV (Figure 6.4), CV (Figure 6.5)
- Interpretation :
  Confidea DI (Figure 6.6), CI (Figure 6.7), 2D2I (Figure 6.8) , DIV (Figure 6.9), CIV (Figure 6.10)

6.2. Controls and indicators

The Confidea WDU have the following features:

1. **Microphone connector**:
   Connection of a microphone to the wireless unit.
2. **Microphone button**:
   Activation/deactivation of the microphone. Indication LEDs show the status of the microphone. (red : active, green : request)
3. **Loudspeaker**:
   Distributes the floor channel. Mutes in case microphone is active.
4. **Headphone connectors:**
   Connection of headphone to the wireless unit. Mono- and stereo headphones can be used.
5. **Volume buttons:**
   Change the volume level of the headphones.
6. **Voting buttons:**
   Each voting button has a blue LED indicator.
7. **Information display:**
   Indication of voting, volume and channel information.
8. **Channel selection buttons:**
   Changes the audio channel sent to the headphones. Each button has a blue indication LED. Pressing these buttons affects the information display.
9. **Voting control buttons:**
   Used by the chairman to control a voting session. (start / pause / stop)
10. **PRIOR button:**
    Long press : temporarily deactivates the microphone of all active units.
    Short press : permanently deactivates the microphone of all active units.
11. **Next button:**
    Grants the floor to the next delegate in the waiting list.
12. **System volume control:**
    Adjust system volume by holding the button and pressing the volume buttons.
13. **RF Status LEDs:**
    Blue LED Indication of the condition of the RF connection.

Off	:	connection established
Blinking	:	searching connection
On	:	out of range

Note:
Units with the out of range LED on will be switched off after 2 minutes.

14. **Battery status LEDs** :
    Red LED blinking the remaining operation time
    1 Hz : 4h remaining
    2Hz : 2h remaining
    4Hz : 1h remaining
15. **Battery connector** :
    (see battery pack – connectors and indicators)
16. **Microphone status LEDs**

Figure 6.1: Confidea DD

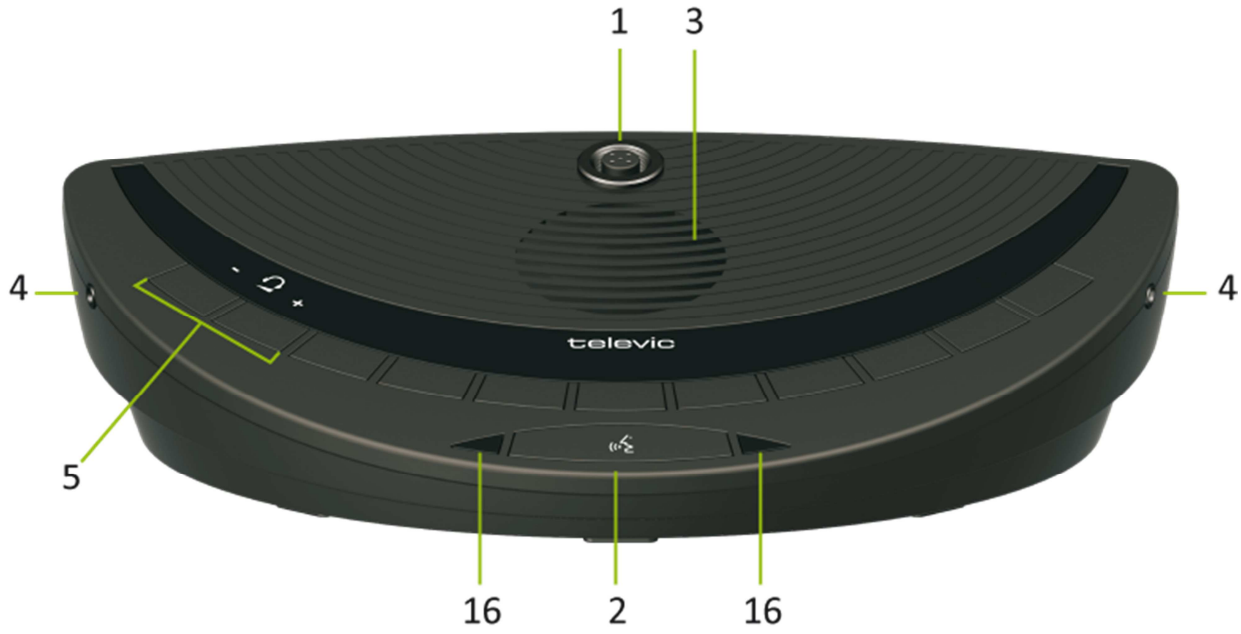


Figure 6.2: Confidea CD

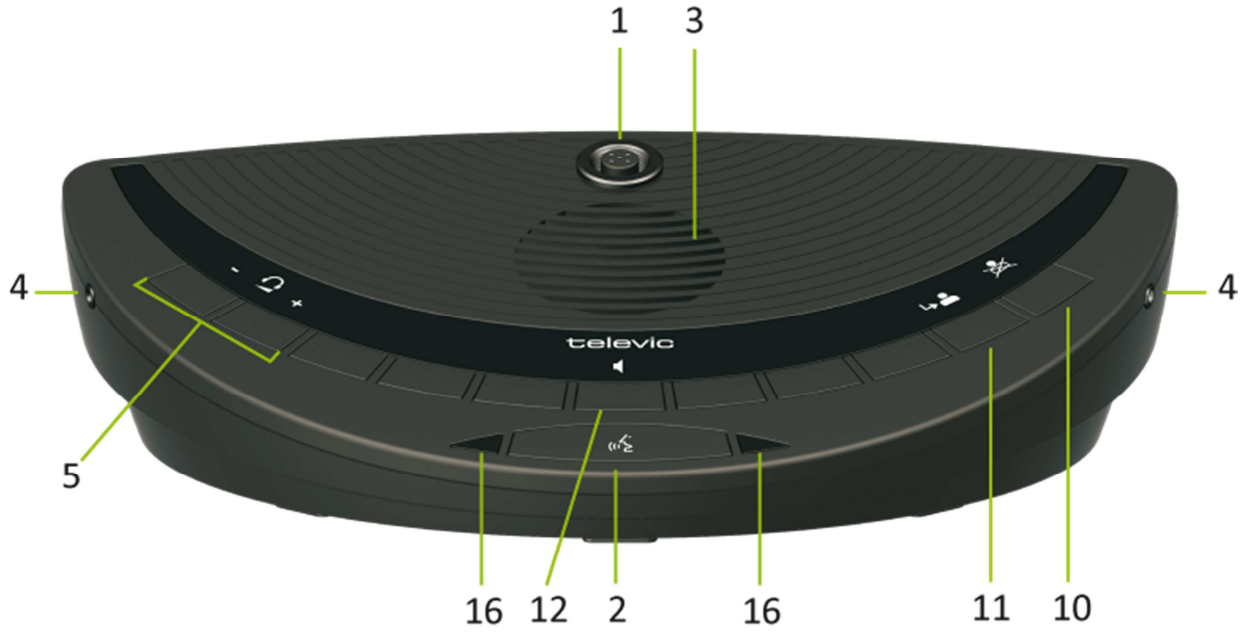


Figure 6.3: Confidea 2D2D

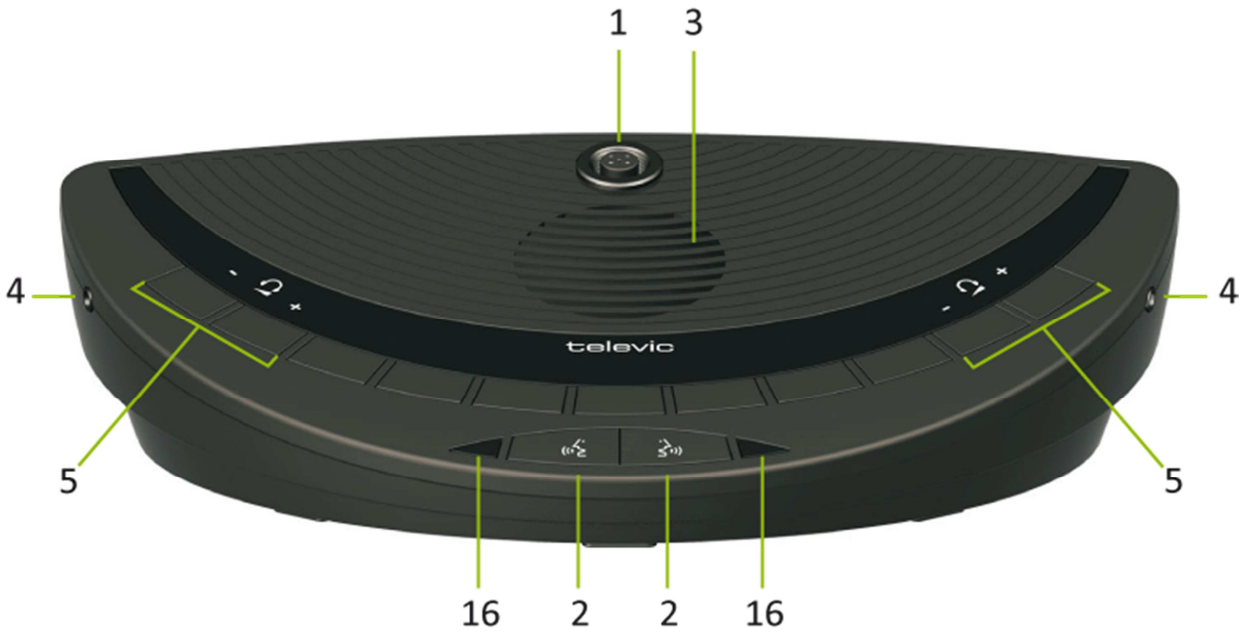


Figure 6.4: Confidea DV

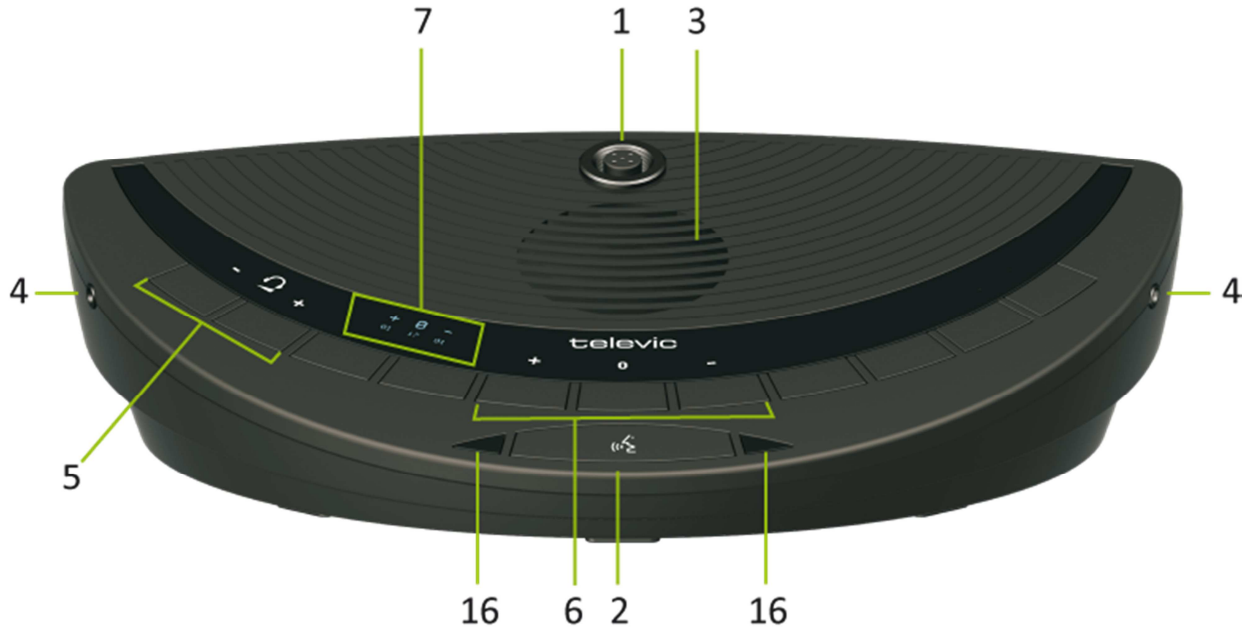


Figure 6.5: Confidea CV

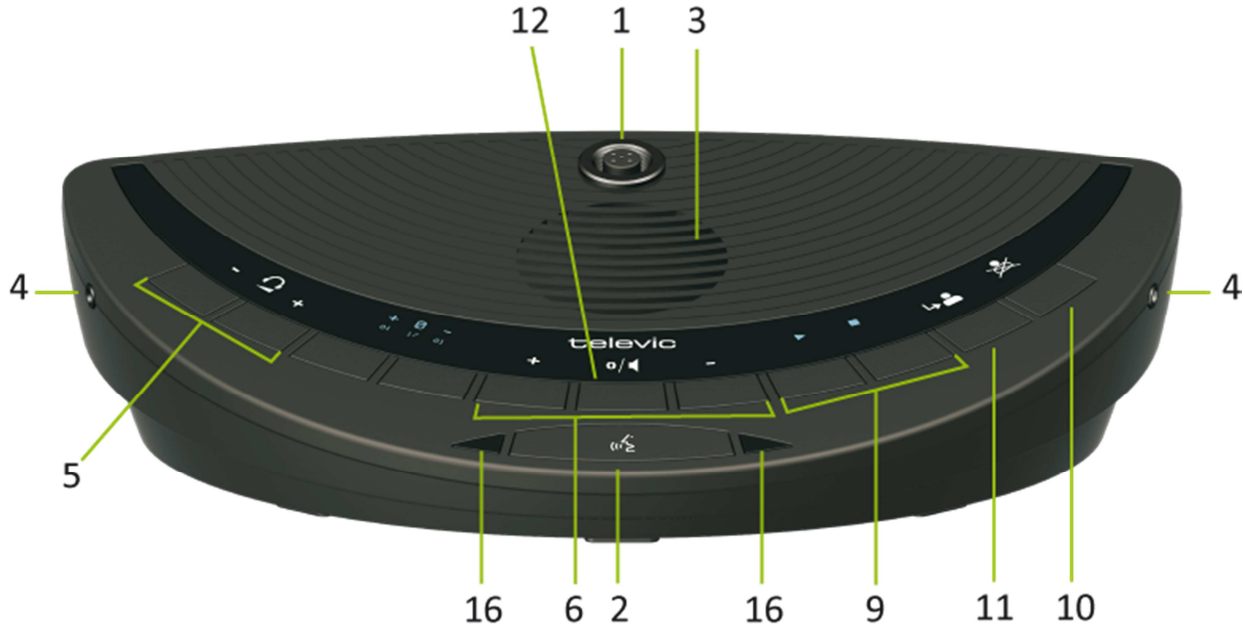


Figure 6.6: Confidea DI

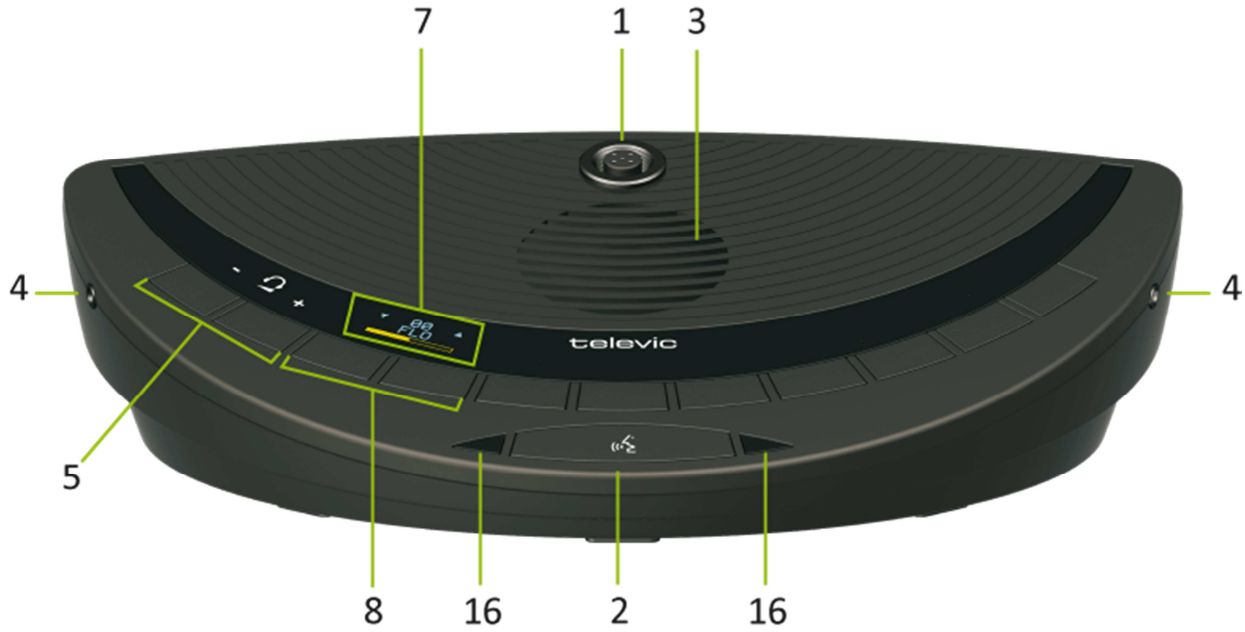


Figure 6.7: Confidea CI

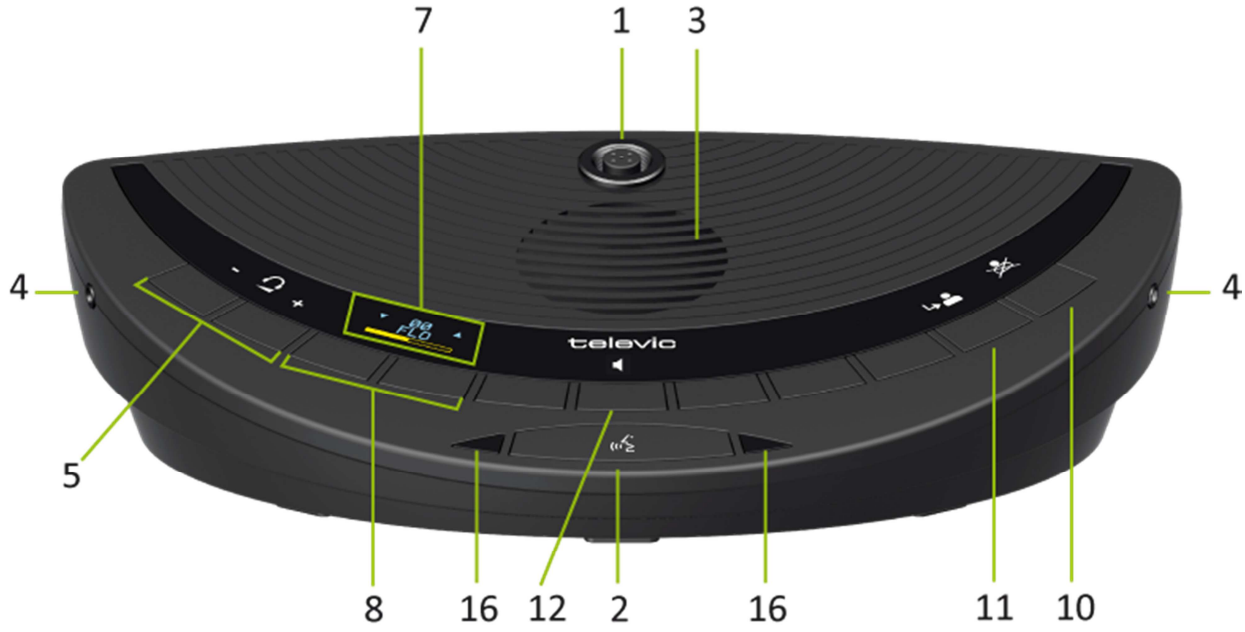


Figure 6.8: Confidea 2D2I

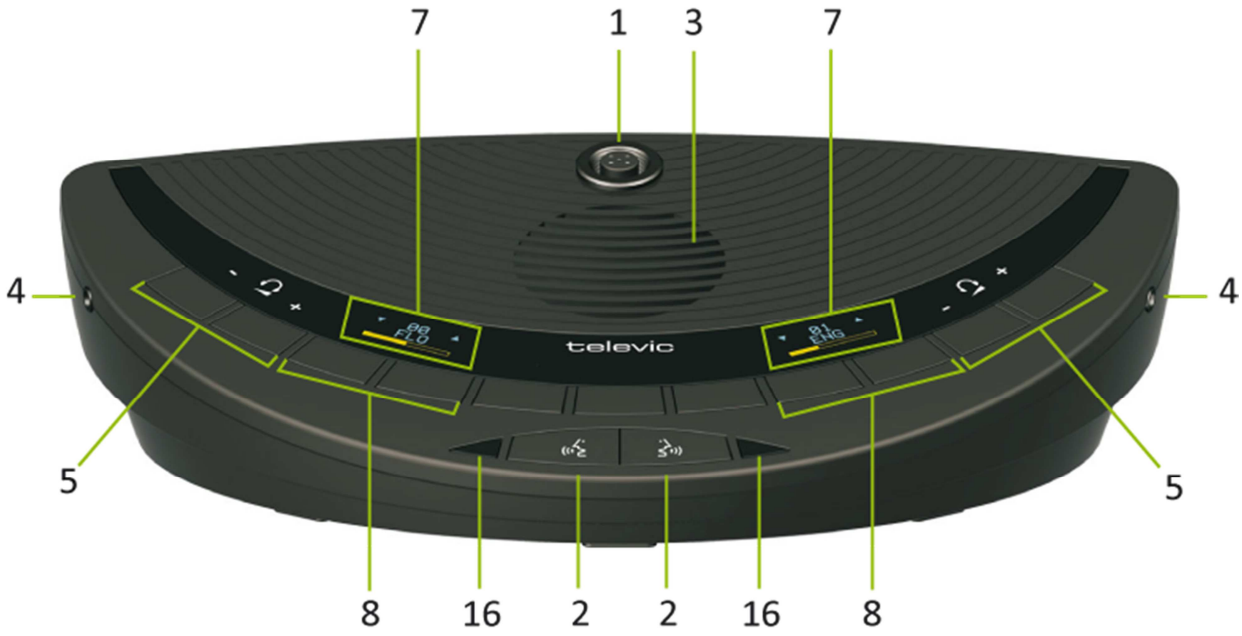


Figure 6.9: Confidea DIV

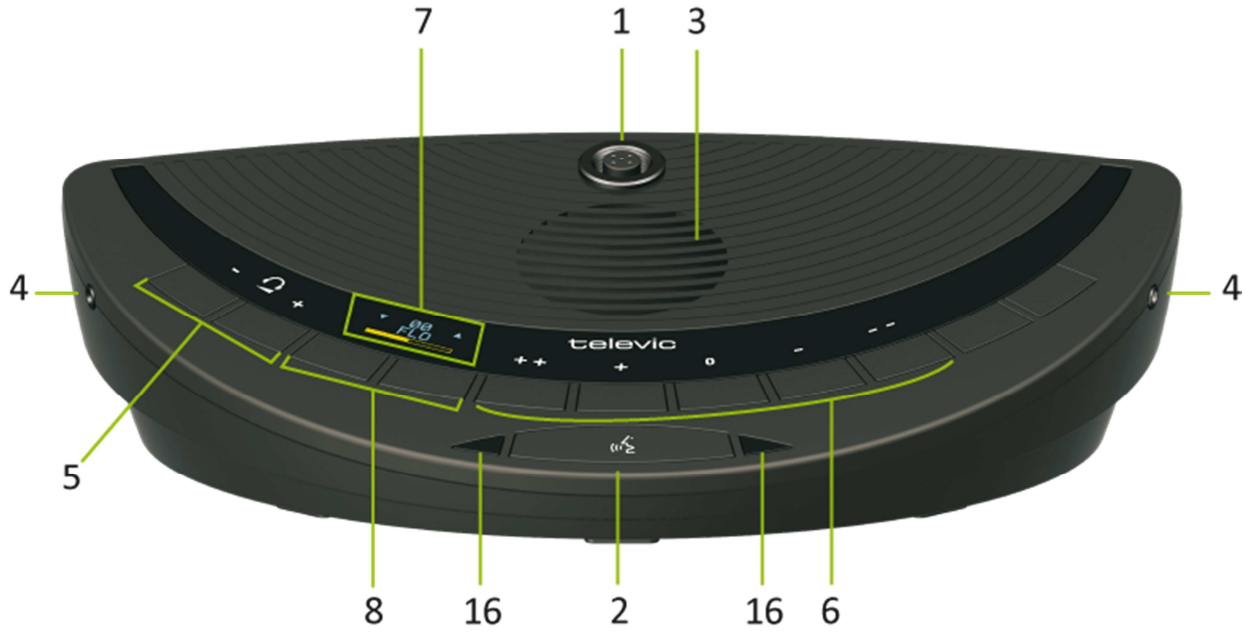


Figure 6.10: Confidea CIV

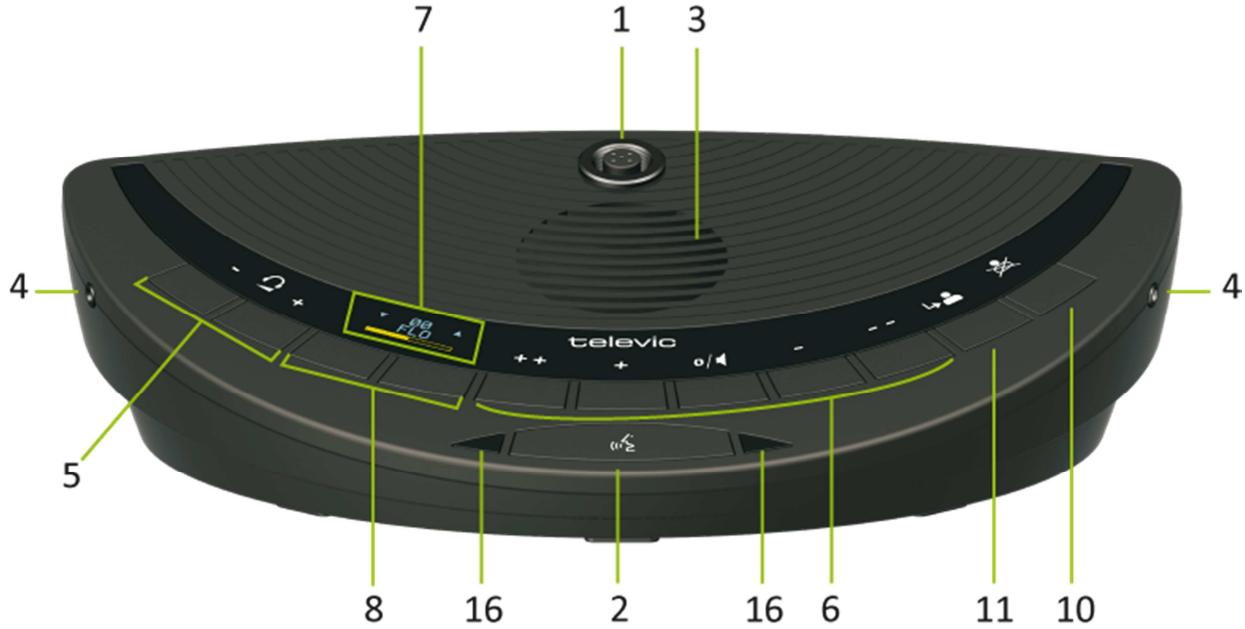


Figure 6.11: RF and Battery Status LEDS

6.3. Installation

In order to use the Confidea WDU, the battery and microphone need to be installed.

For instructions, see the microphone and battery installation and handling chapters. Storage

Disconnect the battery to avoid unwanted operation of the unit. Keep the devices in a clean and dry area.

6.4. Maintenance

6.4.1. General

Caution:
Do not put any objects on top of the units. Object falling through the holes of the unit can cause damage.

Caution:
Do not install the units in a location near heat sources as radiators, air ducts. or direct sunlight.

Caution:
Make sure the units are not exposed to excessive dust, humidity, mechanical vibration or shock.

6.4.2. Cleaning

Caution:
Do not use alcohol, ammonia or petroleum solvents or abrasive cleaners to clean the units.

To keep its original condition it is advised to periodically clean the unit:

- Remove the battery out of the unit.
- Use a clean soft cloth that is not fully moist.
- Make sure the device is completely dry before usage.

6.5. Startup and shutdown of delegate unit

To startup the delegate units simply press shortly on the microphone button.

To shutdown the delegate units , press on the microphone button for 3 sec.

For delegate units with double microphone buttons , switch off/on is done with the right handside microphone button

7. Microphones

7.1. Introduction

The Confidea-MIC38SL (38 cm) pluggable microphone is used with the different delegate- and chairman units. This microphone ha a uni-directional response for optimum performance even in noisy conditions, and has a very low susceptibility to RF-interference from mobile phones.

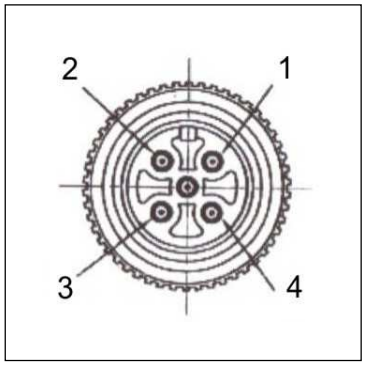
7.2. Electrical and acoustic properties

Table 7.1: Microphone characteristics

Transducer type	Back electret (condenser)
Operating principle	Pressure gradient
Polar pattern	Uni-directional, cardioïd
Frequency response	50 Hz – 16000 Hz
Nominal impedance	1kOhm (at 1 kHz, drop resistance = 1k2, Vdd = 3.3VDC)
Load impedance	> 5kOhm
Max.SPL at 1 kHz	120 dB SPL
Equivalent sound pressure level	< 25 dB(A)
Free field sensitivity	7mV/Pa, +/- 3 dB at 1 kHz or (-43dB, 0dB=1V/Pa at 1kHz)
Power supply	3.3V DC, 0.5 mA
Consumption	0.5 mA (without LED ring); max. 25 mA (with illuminated ring)

7.3. Microphone connector

Figure 7.1: Connector pin layout (bottom view)



- pin 1 : microphone GND
- pin 2 : microphone signal
- pin 3 : unused
- pin 4 : LED +
- pin 5 : LED -

7.4. Operation

The microphone contains the following elements (refer to Figure 7.2):

1. **Indicator ring:** shows the status of the microphone
2. **Union nut:** attaches the pluggable microphone to the unit
3. **Microphone plug:** connects the microphone to the unit

Figure 7.2: Microphone

The colour of the microphone indicator ring shows the status of the microphone (refer to Table 7.2: LED ring status).

Table 7.2: LED ring status

Color	Condition
Red (on)	Microphone active
Red (flash)	Last minute of speech time (if set via software) or Speech request (if set via software)

7.5. Installation and handling

The pluggable microphone has a screw connection. For mounting, plug and fasten the microphone into the unit.

Caution:

Do not force the microphone screw thread while mounting the microphone on the unit .

This can cause permanent damage to the microphone and receptacle connector on the Confidea WDU.

When mount the microphone onto the delegate unit , turn only on the union nut and not on the microphone tube itself , as this can cause permanent damage to the microphone and receptacle connector on the Confidea WDU.

8. Battery Pack

8.1. Introduction

The Confidea wireless battery pack is used with the wireless conference units. Refer to Table 8.1 for the list of compatible devices.

Table 8.1: Compatible devices

Type	Art-nr	Description
Confidea DD	71.98.0001	Delegate Unit
Confidea CD	71.98.0011	Chairman Unit
Confidea 2D2D	71.98.0022	Delegate Unit
Confidea DV	71.98.0002	Delegate Unit
Confidea CV	71.98.0012	Chairman Unit
Confidea DI	71.98.0003	Delegate Unit
Confidea CI	71.98.0013	Chairman Unit
Confidea 2D2I	71.98.0024	Delegate Unit
Confidea DIV	71.98.0004	Delegate Unit
Confidea CIV	71.98.0014	Chairman Unit

Table 8.2: Characteristics

Output voltage:	**7.2V**
Capacity:	6600 mAh
Charge time:	4 Hours
Max charge voltage:	15V
Charge current:	2 A
Autonomy:	+ 20 Hours (Typical)
Dimensions(mm):	172 x 24 x 78

8.2. Safety

Figure 8.1: Battery label 1

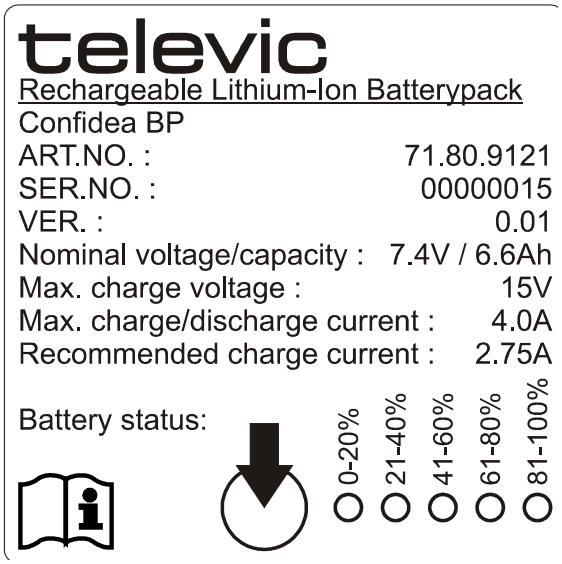
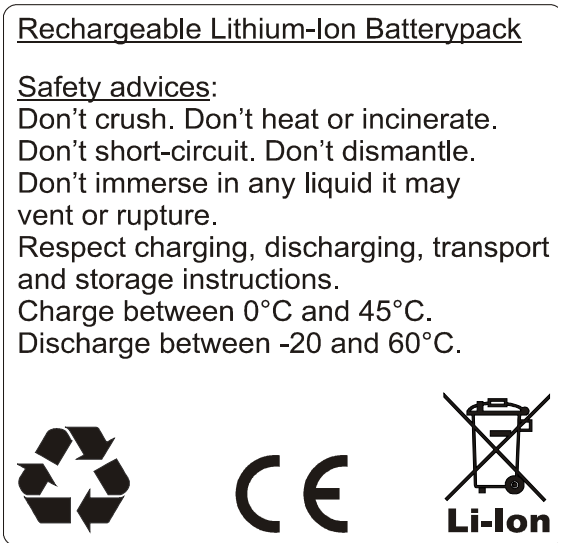


Figure 8.2: Battery label 2


Rechargeable Lithium-Ion Batterypack
Safety advices:
Don't crush. Don't heat or incinerate.
Don't short-circuit. Don't dismantle.
Don't immerse in any liquid it may vent or rupture.
Respect charging, discharging, transport and storage instructions.
Charge between 0°C and 45°C.
Discharge between -20 and 60°C.
Li-Ion

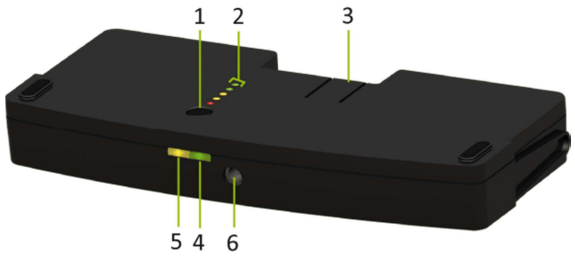
Caution:
To avoid damage, use only the charger supplied by Televic to charge the Confidea Battery Packs.

8.3. Controls and indicators

The battery pack (refer to Figure 8.3) contains:

1. **Test button:**
   Push to check the capacity and the status of the battery pack.
2. **Capacity and status indicator:**
   Shows the capacity of the battery pack (refer to Table 8.3) and the status of the charge circuitry (refer to Table 8.4).
3. **Clip:**
   Locks/unlocks the battery pack in the wireless unit.
4. **Power LED**
   Indicates that the charger is connected and powered.
5. **Charging LED:**
   Indicates the charging status (in progress or completed) when the wall plug battery charger is connected.
6. **Socket**
   To connect the charger plug.

Figure 8.3: Confidea battery pack



8.4. Installation

Install a charged battery pack in a compatible device (refer to Table 8.1).

To check the condition of the battery pack, push the test button 1 (refer to Figure 8.3).

The indicator is a five segment LED. The first LED (LED1 closest to the test button) is red and indicates a low capacity battery. The higher the charge, the higher the number of LEDs that light up.

Table 8.3: Capacity Indicators

LED on	Remaining charge
LED 1 (red)	0-20% (<4hours)
LED 2 (orange)	20-40% (4-8 hours)
LED 3 (orange)	40-60% (8-12 hours)
LED 4 (green)	60-80% (12-16 hours)
LED 5 (green)	80-100% (16-20 hours)

Note:
The battery capacity as listed in Table 8.3 has an accuracy of 20%.

After the display of the battery condition (for 4-5 seconds), the first three LEDs (LED1 to LED3) will indicate the status of the charge circuitry (refer to Table 8.4).

Table 8.4: Charge circuitry status

LED 3 is flashing:	Charging circuitry is ok
All other indications:	Indicates a failure Disconnect the charger from the battery pack and remove the battery pack from the conference unit.

To charge a battery pack, refer to chapter 9.3 ‘Charging a battery pack’.

8.5. Storage and discharge behaviour

Lithium ion cells self-discharge very slowly giving them long shelf life.

Although the battery packs are protected against unwanted self discharge it is advised to read the following note concerning Li Ion battery pack storage.

Note:

Store at low temperature

Store at 50% charge

Remove from unit for long term storage

To maximize shelf life of your Li-Ion battery pack, please take into account the following guidelines:

8.5.1. Store at low temperature

Storage temperature has the highest effect on self-discharge. Higher temperatures increase self discharge (Fig.1). Storage of cells and batteries in non-temperature controlled facilities in hot climates can cause quicker self discharge. Hence the storage conditions affect the shelf life of the product

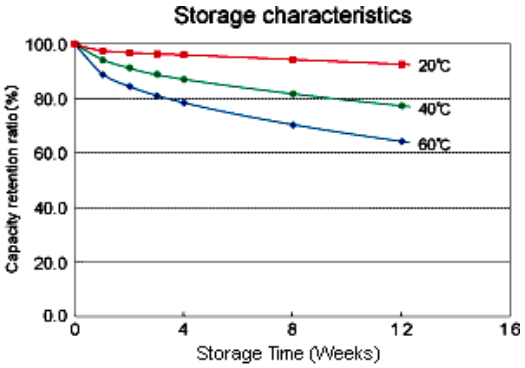


Fig. 8.5.1: Capacity degradation as a function of temperature

8.5.2. Store at 50% charge

For maximum lifetime, we recommend to charge the battery to approximately 50% of its capacity before storing it for a long period of time

8.5.3. Remove from unit for long term storage

For long term storage, we recommend to remove the Confidea® battery from the conference unit, even if the unit is switched off. As indicated in fig 2. and fig.3, self discharging rate of the battery can be reduced to approximately 1/3 when the battery is removed from the unit

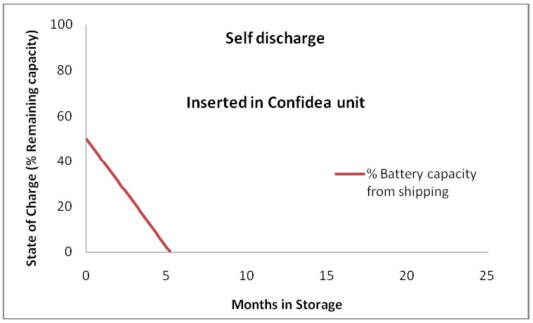


Fig. 8.5.3.1: Self discharge - inserted in Confidea WDU

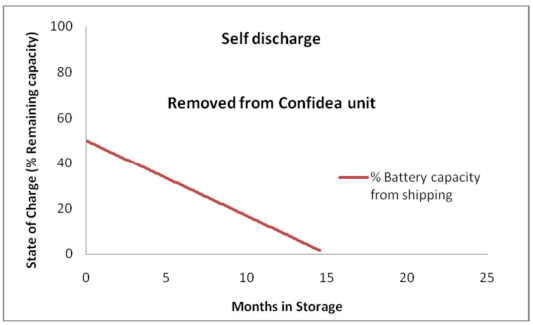


Fig. 8.5.3.1: Self discharge - removed from Confidea WDU

9. Wall plug battery charger

9.1. Introduction

Use the supplied wall plug battery charger to charge the battery pack used with wireless conference units. Refer to Table 9.2 for the compatible battery packs.

Table 9.1: Electrical properties

Input:	90-264V(AC) 50-60Hz
Output:	15V(DC), 2A

Caution:
To avoid damage, use only the charger delivered by Televic to charge the Confidea Battery Packs.

Table 9.2: Compatible battery packs

Type	Art-nr	Description
Confidea BP	71.80.9121	Rechargeable Lithium-ion battery pack.

9.2. Installation

Installing the plug of your need can be done by simply sliding one of the interchangeable plugs on the battery charger. (refer to Figure 9.1)

Figure 9.1:Wall plug battery pack

9.3. Charging a battery pack

Connect the wall plug battery charger to the socket (6) of the battery pack (refer to Figure 8.3). The Power LED lights up (refer to Table 9.3).

During the charge, the charging LED is lit, and the capacity indicator shows the capacity of the battery pack. The top LED segment of the capacity indicator flashes (e.g.: if state of charge = 36% then LED2 will blink). Pushing the test button has no effect when the charge is in progress.

When the charging is completed, the charging LED (5) and the capacity indicator (2) switch off. Push the test button (1) to check the capacity of the battery pack. The LED segment indicator will show the capacity of the battery for a few seconds, then the status of the battery (refer to chapter 8.4 'Installation') will be indicated.

Note:
A battery pack can be charged separately, or when inserted in a wireless unit.

Note:
The wall plug charger can be used to power a Confidea wireless unit. In this case the battery pack needs to be installed in the unit.

Table 9.3: Charging status indicators

Status	Power LED (green)	Charging LED (yellow)	Capacity indicator
Charge is in progress	On	On	On (top LED segment flashes)
Charge is completed	On	Off	Off (Push test button to check the capacity and the status)
Charger is disconnected or not powered	Off	Off	Off (Push test button to check the capacity and the status)

9.4. Use of battery charging tray

Type	Art-nr	Description
Confidea CHT	71.98.0043	Confidea wireless Charging Tray. Can be mounted in 19” rack

Figure 9.4:Battery charging tray

Each battery charging tray can charge up to 6 battery packs simultaneously.

Mains AC supply	Max number of CHT connected in daisy chain
110 – 125V	3
220 - 240V	8

Caution:
To avoid damage, or overheating , Confidea Charging Trays may not be covered while batteries are plugged in!

10. Wireless Conference Access Point (WCAP)

10.1. Introduction

All communication to and from the wireless units is controlled by the WCAP.

10.2. Installation

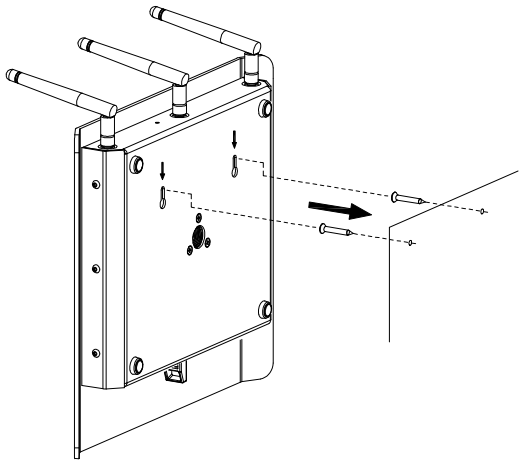
10.2.1. General

Caution:
Do not open the wireless access point. Opening the wireless access point may cause permanent damage to the device. Opening WCAP is only allowed by qualified personnel.

10.2.2. Wall Mounting

The WCAP can be mounted on the wall by means of the 2 fixing holes at the bottom side of the device

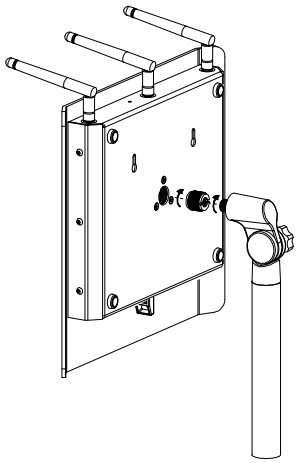
Figure 10.1: Wall mounting



10.2.3. Tripod Mounting

The WCAP can also be mounted on a tripod.

Figure 10.2: Tripod mounting

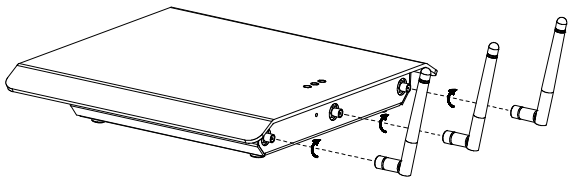


10.2.4. Antennas

The WCAP has 3 antennas which can be positioned in different directions independent from each other.

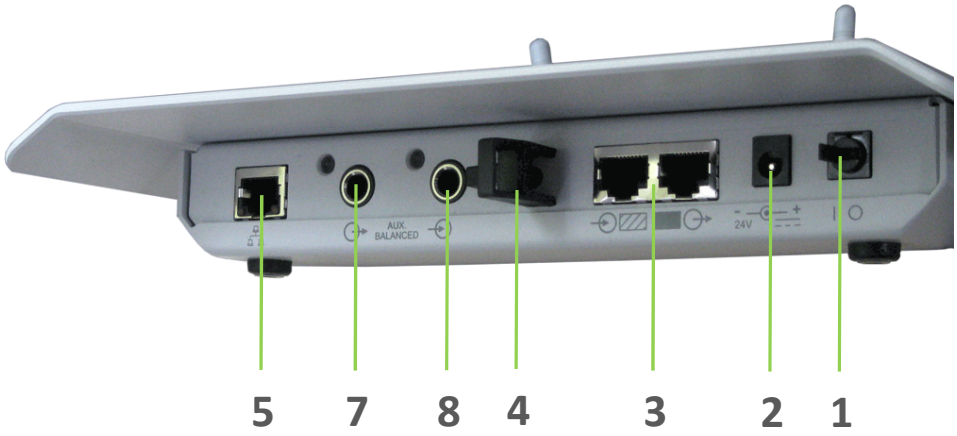
Caution:
Only use antennas supplied by Televic. Use of other antennas can cause damage to the unit and reduce system performance.

10.3: Antenna mounting



10.3. Connections and Controls

Figure 10.4: WCAP connections



1. **Power Switch**
   The WCAP can be switched on/off with the power switch at the back of the WCAP.
2. **Power Supply**
   The power supply for the wireless delegate units is provided by batterypacks (see also chapter 8)
   The power supply of the WCAP is provided by a 230VAC/24VDC adaptor
   The WCAP can also be powered by a central unit CPU5500(48VDC) or by connecting it to a SPL5525. In both cases no separate power supply is needed .
3. **Digital Bus Connection**
   The Connection with the Televic digital conference bus is done through RJ45-connectors at the back of the WCAP. Connections can be made to Confidea CU or SPL5525.
4. **Cable retention clip**
   The cable retention clip is used to safegard the cable of the power adaptor
5. **LAN port**

   Through the LAN connector at the back of the WCAP, a PC can be connected using a standard cat. 5e FTP network cable.
6. **Status LEDS**
   The status LEDs give information on selected mode, RF link quality (Signal/Noise Ratio) and delegate unit detection

   (see fig.10.5 , table 10.1 …3 for hardware version 0.01 and table 10.4…6 for hardware version 0.02)
7. **Aux input**

   Auxiliary balanced input connector
8. **Aux output**

   Auxiliary balanced output connector

Figure 10.5: LED indicators

Hard ware version 0.01

Table 10.1: LED 1 (Blue) - Mode

OFF	No connection
SLOW BLINKING	Slave mode Confidea CU
BLINKING	Slave Mode TCS5500
ON	Standalone mode

Table 10.2: LED 2 (Red) - RF link quality

OFF	RF LINK OK
SLOW BLINKING	$10<SNR_{AVG}<15$
BLINKING	$5<SNR_{AVG}<10$
ON	$SNR_{AVG}<5$

Table 10.3: LED 3 (Blue) - Status

BLINKING	No units initialized
ON	At least 1 unit has been connected with the WCAP

All 3 LEDs blincking simultaneously indicate network errors (e.g. wrong slave setting)

Hardware version ≥ 0.02

Table 10.4: LED 1 - Mode

ON	Stand alone mode
BLUE BLINKING	Slave mode Confidea CU
GREEN BLINKING	Slave Mode TCS5500

Table 10.5: LED 2 (Red) - RF link quality

OFF	RF LINK OK
SLOW BLINKING	$10<SNR_{AVG}<15$
BLINKING	$5<SNR_{AVG}<10$
ON	$SNR_{AVG}<5$

Table 10.6: LED 3 (Blue) - Status

BLINKING	No units initialized
ON	At least 1 unit has been connected with the WCAP

All 3 LEDs blincking simultaneously indicate network errors (e.g. wrong slave setting)

Section 3 – System Configuration

11. Accessing the built-in web server

11.1. Introduction

The *WCAP* has a built-in web server that allows you to set/monitor certain parameters characterizing the wireless conference system.

The following is a step-by-step guide to give you a general idea of how to access your WCAP.

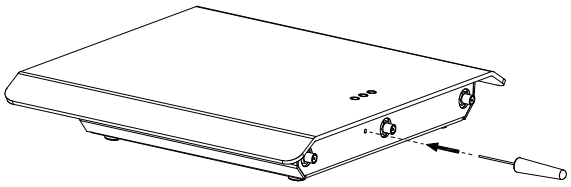
11.2. First time access

11.2.1. Step 1 – Reset

Note:
This step is only required if the default settings have been altered.

Figure 11.1: Power connection and power switch

Figure 11.2: Reset button



Follow these steps to reset the access point (WCAP)

- Unplug ALL connections
- Connect the power cord
- Activate the *WCAP* by flipping the power switch to the “on” position
- Hold down the reset button for at least 5 seconds using a fine object or stylus.
- Using the ON/OFF switch, switch the unit “off” and back “on” for the reset to take effect

After the reset the default settings in the *WCAP* will be restored. Please refer to Default Settings to get a complete overview of all default settings.

11.2.2. Step 2 – PC or MAC TCP/IP setup

Note:
The *WCAP* has a default fixed IP address and subnet mask:

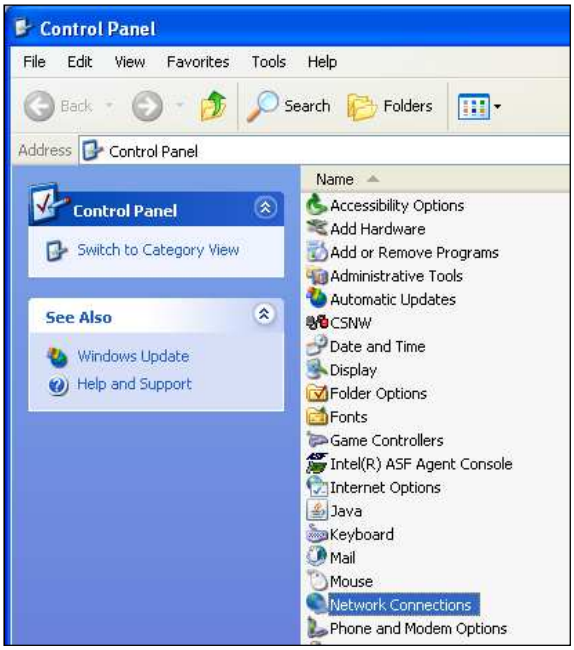
- IP: 192.168.0.10
- Subnet mask: 255.255.255.0

In order to access the built-in web server for the first time, the TCP IP settings from the PC or MAC must be modified. A fixed IP address has to be set. Therefore follow the instructions below.

Assigning a Static IP Address in *WINDOWS XP/2000*

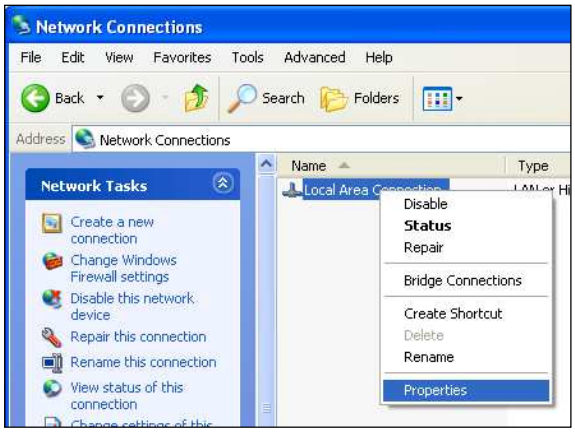
- Go to the ' Control Panel' (refer to Figure 11.3)
- Double-click on Network Connections

Figure 11.3: Control Panel



- Right-click on Local Area Connection (refer to Figure 11.4).
- Double-click on Properties

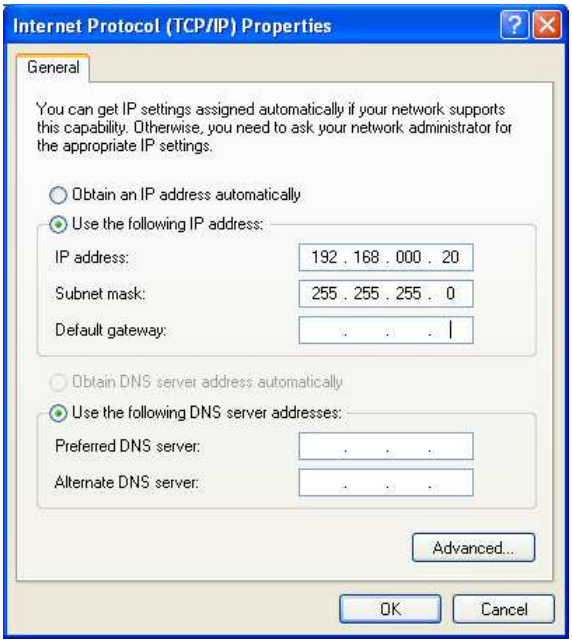
Figure 11.4: Network Connections



- Click on Internet Protocol (TCP/IP)
- Click Properties
- Input your IP Address and subnet mask (refer to Figure 11.5).
  The IP Addresses on the network must be within the same range. The default IP address from the WCAP is 192.168.0.10 so the computer should have an IP Address that is within the same subnet, like 192.168.0.11 and 192.168.0.20. The subnet mask must be the same for all equipment on the network: 255.255.255.0)
- Click OK

Note:
Be sure not to use the IP address 192.168.0.10 for your computer, as this is reserved and used by the WCAP as a default.

Figure 11.5: TCP/IP properties

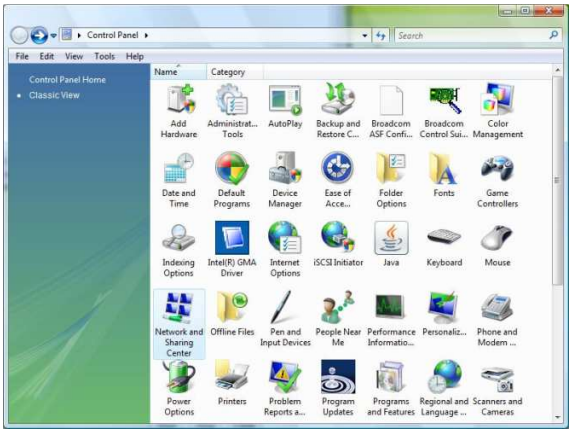

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 000 . 20
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Assigning a Static IP Address in *WINDOWS VISTA*

– Go to the ‘ Control Panel’ (refer to Figure 11.3)

– Double-click on Network and Sharing Center

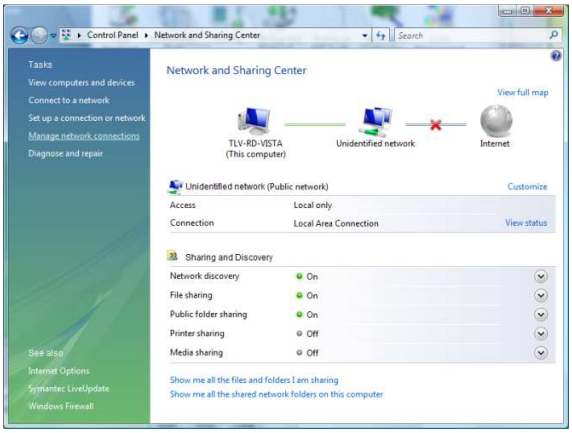
Figure 11.6:Control Panel



– Click on Manage Network Connections

(refer to Figure 11.3)

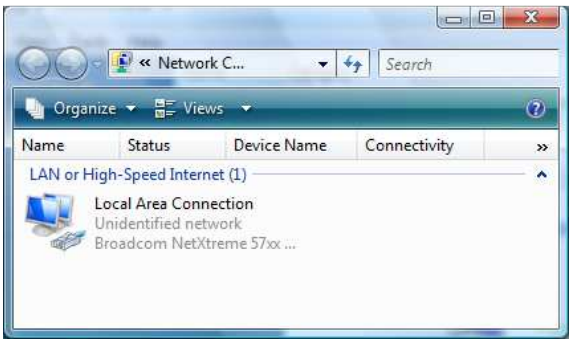
Figure 11.7:Netwerk and Sharing Center



– Right-click on Local Area Connection (refer to Figure 11.8: Local Area Connection).

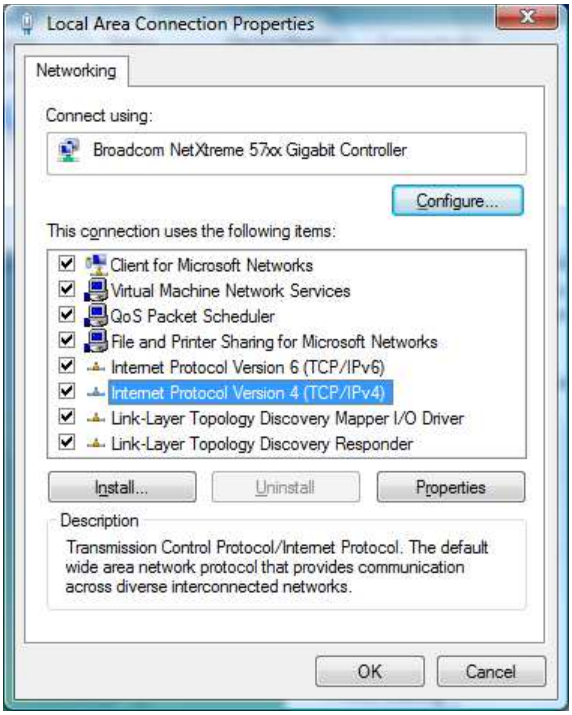
– Double-click on Properties

Figure 11.8: Local Area Connection



– Click on Internet Protocol (TCP/IP) (refer to Figure 11.9 : Local Area Connection Properties).

Figure 11.9 : Local Area Connection Properties



– Click Properties

– Input your IP Address and subnet mask (refer to Figure 11.5).
The IP Addresses on the network must be within the same range. The default IP address from the WCAP is 192.168.0.10 so the computer should have an IP Address that is within the same subnet, like 192.168.0.11 and 192.168.0.20. The subnet mask must be the same for all equipment on the network: 255.255.255.0)

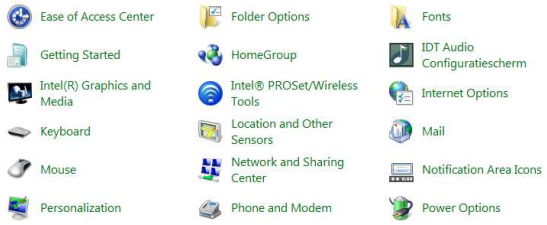
– Click OK

Assigning a Static IP Address in *WINDOWS 7*

- Go to 'Control Panel' (refer to Figure 11.10:Control Panel0)

- Double-click on Network and Sharing center

Figure 11.10:Control Panel

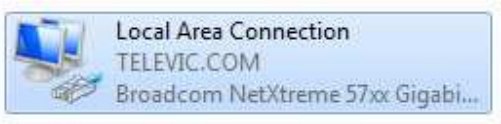


- Click on Change adapter settings
(refer to Figure 11.11: Netwerk and Sharing)

Figure 11.11: Netwerk and Sharing

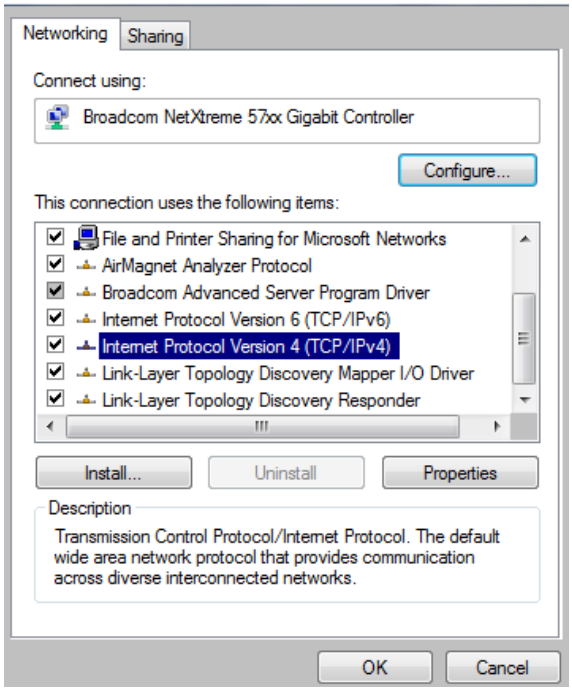
- Right-click on Local Area Connection (refer to Figure 11.12: local Area Connections)
- Click on Properties

Figure 11.12: local Area Connections



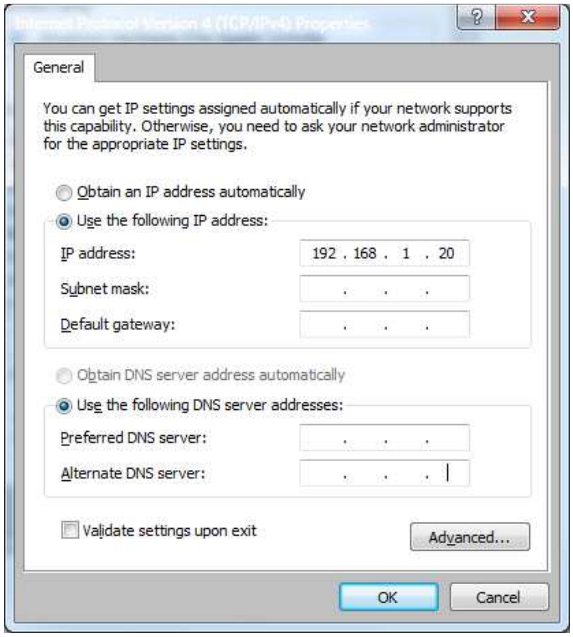
- Click on Internet Protocol 4 (TCP/IPv4) (refer to Figure 11.13: Local Area Connections Properties).

Figure 11.13: Local Area Connections Properties



- Click properties
- Input your IP Address and subnet mask (refer to Figure 11.14: TCP/IP Properties). The IP Addresses on the network must be within the same range. The default IP address from the WCAP is 192.168.1.111 so the computer should have an IP Address that is within the same subnet, like 192.168.0.11 and 192.168.0.20. The subnet mask must be the same for all equipment on the network: 255.255.255.0)
- Click OK

Figure 11.14: TCP/IP Properties


General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 20
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Assigning a Static IP Address with *MACINTOSCH OSX*

- Go to the Apple Menu and select System Preferences
- Click on Network
- Select Built-in Ethernet in the Show pull-down menu
- Select Manually in the Configure pull-down menu
- Input the Static IP Address and the Subnet Mask Address in the appropriate fields. (The IP Addresses on the network must be within the same range. The default IP address from the WCAP is 192.168.0.10 so the computer should have an IP Address that is sequential, like 192.168.0.11 and 192.168.0.20. The subnet mask must be the same for all equipment on the network: 255.255.255.0)
- Click Apply Now

Note:
If you have a proxy server or firewall installed on your computer check the connection restrictions to the *WCAP* IP address and content that uses java scripts.
Please refer to the documentation that came with your installation for the correct settings.

Reference:
Please refer to the documentation that came with your PC or MAC installation for additional information and the correct settings.

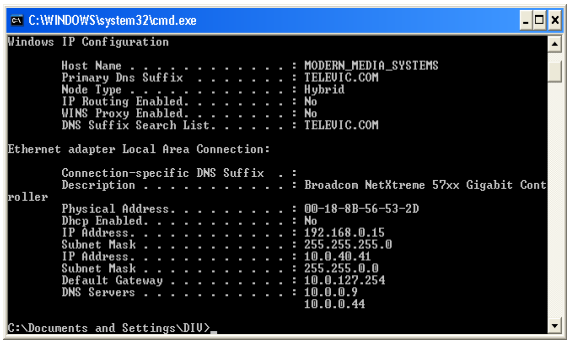
Assigning multiple IP Addresses *(IP – Aliasing)*

To use multiple tcp_ip addresses on your PC , set a fixed IP address first as explained above and add the appropriate Subnet Mask , Default Gateway and the DNS server addresses.

The Default Gateway and DNS servers can be determined by executing the command *ipconfig /all* in a "cmd" screen

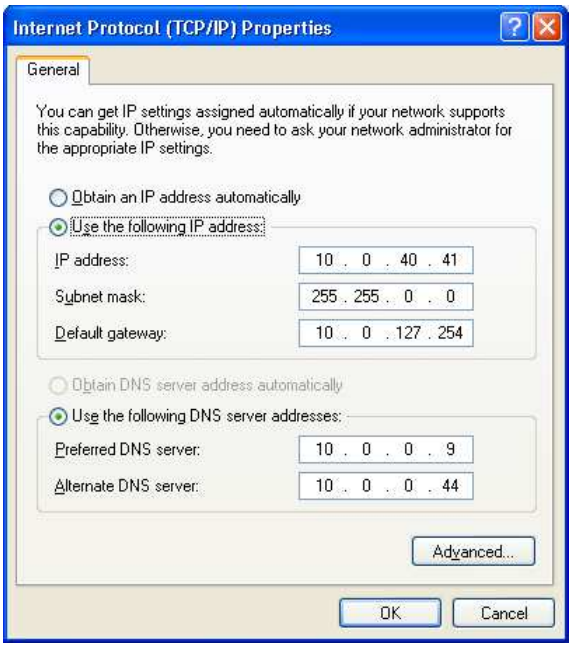
Windows XP : click on Start > RUN > cmd
Windows Vista : click on Start > All Program Files > Accessories > Command Prompt
(refer to Figure 11.15 : Command prompt).

Figure 11.15 : Command prompt


C:\WINDOWS\system32\cmd.exe
Windows IP Configuration
Host Name . . . . . : MODERN_MEDIA_SYSTEMS
Primary Dns Suffix . . . . . : TELEVIC.COM
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : TELEVIC.COM
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : Broadcom NetXtreme 57xx Gigabit Controller
Physical Address. . . . . : 00-18-8B-56-53-2D
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.0.15
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : 10.0.40.41
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.0.127.254
DNS Servers . . . . . : 10.0.0.9
10.0.0.44
C:\Documents and Settings\DIV>

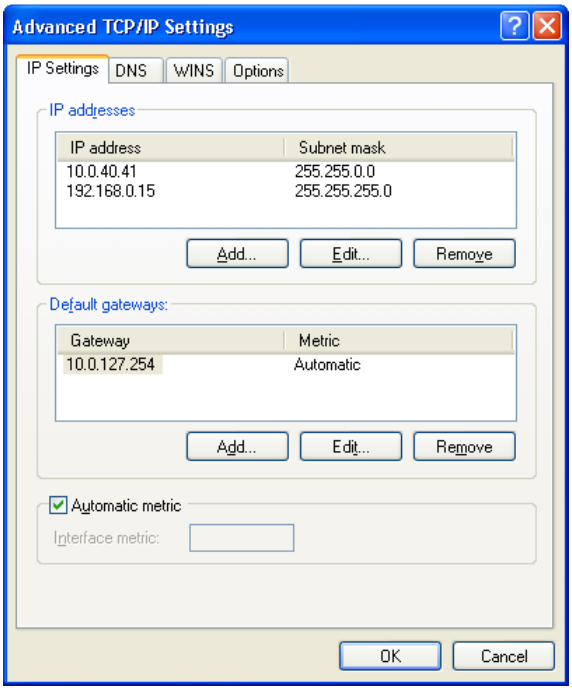
In this example the PC has normally "10.0.40.41" as IP address. Now IP Address "192.168.0.15" (e.g.) has to be added to be able to access the web-server of the WCAP.

Figure 11.16 : DNS and Gateway settings


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 40 . 41
Subnet mask: 255 . 255 . 0 . 0
Default gateway: 10 . 0 . 127 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 10 . 0 . 0 . 9
Alternate DNS server: 10 . 0 . 0 . 44
Advanced...
OK
Cancel

Next click on "Advanced" and "Add"… to add IP Address(es) and click 2x OK. (refer to Figure 11.17: Adding IP-Addresses).

Figure 11.17: Adding IP-Addresses

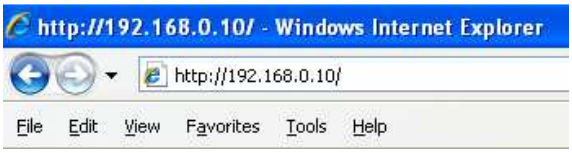


11.2.3. Step 3 – Cable Setup

Connect your computer (PC or MAC) to the LAN port using a straight-through patch cable.

11.2.4. Step 4 – Accessing WCAP

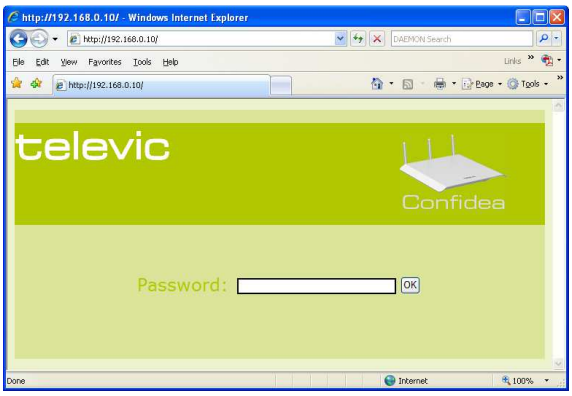
Figure 11.14 : Internet Explorer address bar



– Open Internet Explorer or any other browser (with the computer connected to the *WCAP*)

– Enter 192.168.0.10 into the Address Bar, push Enter

Figure 11.15: WCAP password page



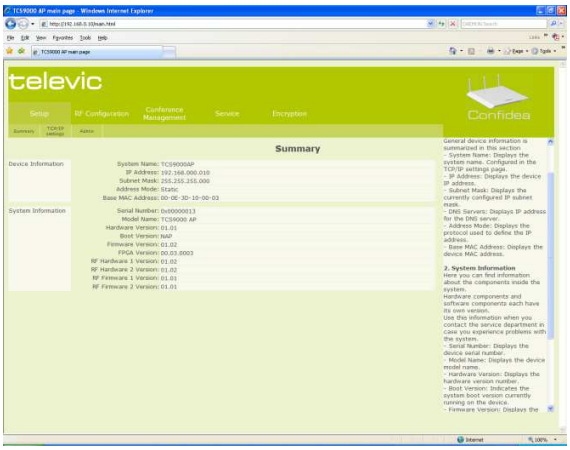
– The Default Password is “123”

– Click “OK”

11.2.5. Step 5 – Default Screen

After successfully establishing a connection to the WCAP and passing the password screen, the default WCAP screen appears.

Figure 11.18 : WCAP default screen



Note 11.2-1

Confidea wireless webserver has been fully tested successfully on Windows Internet Explorer 8 .

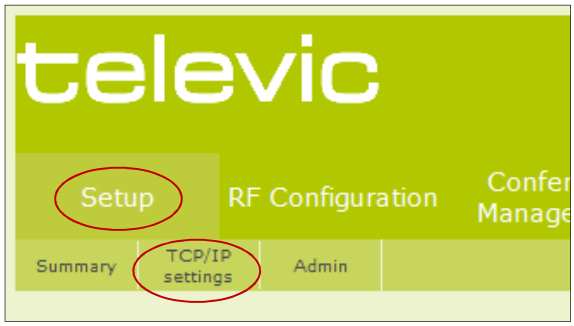
However , since there exists a wide variaty of web browsers , which are subject to regular updates , 100% correct functionality of Confidea wireless webserver on all browser types can not be guaranteed, because some actions may be blocked by specific browsers.

11.3. Setting the IP address

After you successfully accessed the *WCAP* for the first time (refer to 11.2 'First time access') you can customize the TCP/IP settings to allow the *WCAP* into your own personal or company LAN network.

– Select the "TCP/IP settings" sub tab in the "Setup" menu (refer to Figure 11.19: Confidea wireless setup menu)

Figure 11.19: Confidea wireless setup menu



– In the TCP/IP settings - screen you can modify the TCP/IP settings of the *WCAP* (refer to Figure 11.20).

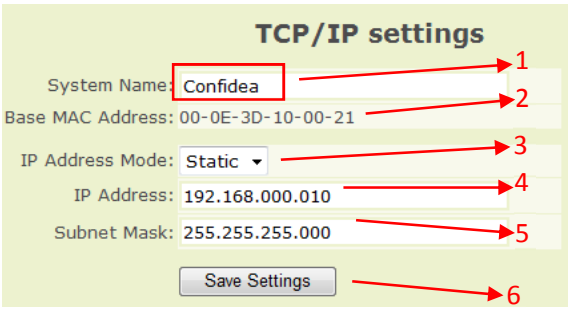
1. The name of the installed conference system can be customized.
2. The MAC address of the WCAP (fixed)
3. The IP address mode determines how the *WCAP* will get its IP address
   – Static: in this mode the IP address and subnet mask is fixed and must be provided in the appropriate fields.
   – DHCP: DHCP stands for Dynamic Host Configuration Protocol and is a protocol used by the WCAP to obtain the parameters necessary for operation in an Internet Protocol network automatically. This protocol reduces system administration workload, allowing the WCAP to be added to the network with little or no manual configuration.

Note:
There must be a DHCP server on the network that dynamically assigns IP addresses when using the DHCP setting.

4. Here you can enter the desired fixed IP address. Only applicable in fixed IP address mode.
5. Here you can enter the desired subnet mask. Only applicable in fixed IP address mode.
6. Press this button to save the modified values.

Note:
The new TCP/IP settings will only be active after repowering the *WCAP*

Figure 11.20: Screen TCP/IP settings



11.4. Updating SW

After first startup it is advised to check if there are SW updates available on the Televic website:

http://www.televic-conference.com/en/confidea_wcap?tab=207

Unzip the files to a location on your hard drive where you can easily find them back **.**

Switch on the Confidea Access Point and all wireless Confidea WDUs that need updating.

With a regular internet browser, go the Access Point web server . (see also Note 11.2-1

To perform a SW update select the Service – Update screen

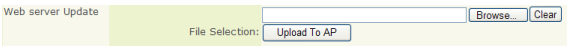
Figure 11.21: Update screen

The configuration index is to be left at “1” (default).

SW update must be done in the following order:

Note:
Only files that have changed need to be uploaded.

Step 1:
In the Web Server Update screen , browse to and select the "webrombin.bin" file to update the webserver.



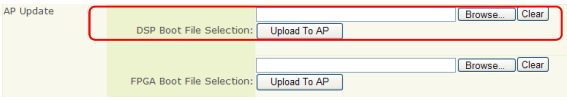
Select "upload to AP". A green progress bar appears at the bottom of the screen and after +/- 5 sec the screen is refreshed.

Upload is finished.

Note:
Depending on the used webbrowsertype and version , the progressbar may not always be visible.

Step 2:

In the AP Update screen , browse to and select the DSP Bootfile "firmware_ap.bin" file to update the AP.
Select "upload to AP".

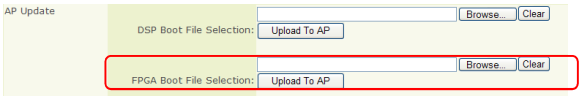


A green progress bar appears at the bottom of the screen and after +/- 5 sec the screen is refreshed.
Upload is finished.

Note:
Depending on the used webbrowsertype and version , the progressbar may not always be visible.

Attention : The name of the file must be exactly " firmware_ap.bin "

Step 3: In the AP Update screen , browse to and select the FPGA Bootfile "vhdl_ap.bin" file to update the AP.



Select "upload to AP". A green progress bar appears at the bottom of the screen and after +/- 5 sec the screen is refreshed.
Upload is finished.

Note:
Depending on the used webbrowsertype and version , the progressbar may not always be visible.

Attention : The name of the file must be exactly " vhdl_ap.bin "
A reboot op the Confidea Accesspoint is needed to activate the new SW version : Select "Reboot AP".

Step 4:
After the AP update procedure , it is advised to perform a full reset : press the reset button next to the middle antenna during 5 sec. and release it. (this will also reset the ip address to the default value)

After the update all AP setting. (country, RF, conference,...) need to be reconfigured

Note:

During the update it is possible that the stylesheet for the web pages are not loaded correctly. After the complete update this will be fixed.

If the connection is lost after a failed update session then the hard coded web server link has to be used to proceed with the update.

http://192.168.0.10/sublinks/update_main_gold.shtml

Note:

After updating the WCAP SW , check through the webserver "summary" section, if the SW update has been successfull, as some types of anti-virus SW and/or firewall restrictions may block the updates of the WCAP SW.
If needed disable the anti-virus SW for the duration of the WCAP SW update.

Caution:

Before starting SW update of WDU, make sure the batteries of ALL WDU's are charged up to at least 20% !

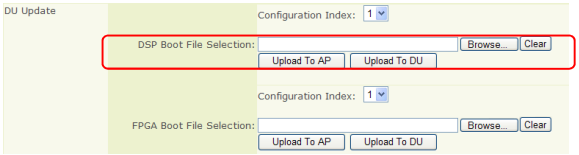
During WDU SW update procedure do not move any WDU's !

Updating SW of WDU's with insufficient batterycharge or while WDU's are moved around may result in slowdown of or even failed update procedure !

Step 5:

First check if all units are connected via the "Conference Management -> Unit Monitoring" tab.

In the DU update screen , browse to and select the " firmware_ wdu.bin " file to update the DSP boot file of the delegate unit.



First the file needs to be uploaded to the AP ("select Upload to AP"). A green progress bar appears at the bottom of the screen and after +/- 5 sec the screen is refreshed.

Note:
Depending on the used webbrowsertype and version , the progressbar may not always be visible.

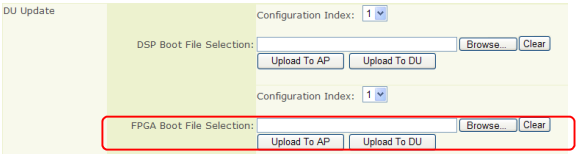
Then the file needs to be uploaded from the AP to the DU (select “Upload to DU”).
Following message appears :

Followed by a progressbar after pressing “OK” :

Attention : The name of the file must be exactly “ firmware_ wdu.bin ”

Step 6:

In the DU updatescreen , browse to and select the “vhdl_wdu.bin” file to update the FPGA boot file (*) of the delegate unit.



First the file needs to be uploaded to the AP (“select Upload to AP”).
Then the file needs to be uploaded from the AP to the DU (select “Upload to DU”).

Attention : The name of the file must be exactly “ vhdl_wdu.bin ”

A reboot op the DU’s is needed to activate the new SW version : Select “Reboot DU’s”

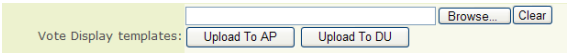
(*) Remark : if an update of both DSP and FPGA file is needed , the WDUs may only be rebooted after **both** files have been uploaded.

Caution:

Do not switch off the Confidea Wireless Access Point or any of the Confidea wireless Delegate Units while the upload is in progress.

Step 7:

In the DU updatescreen , browse to and select the “vote_display.bin” file to update the voting display templates (*) of the delegate unit.



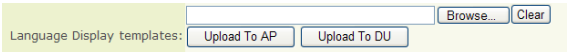
First the file needs to be uploaded to the AP (“select Upload to AP”).
Then the file needs to be uploaded from the AP to the DU (select “Upload to DU”).

Attention : The name of the file must be exactly “ vote_display.bin ”

(*) Remark : uploading vote display templates is only needed for delegate units with WDU SW 1.12 or older .

Step 8:

In the DU updatescreen , browse to and select the “language_display.bin” file to update the language display templates (*) of the delegate unit.



First the file needs to be uploaded to the AP (“select Upload to AP”).
Then the file needs to be uploaded from the AP to the DU (select “Upload to DU”).

Attention : The name of the file must be exactly " language_display.bin "

A reboot op the DU's is needed to activate the new templates : Select "Reboot DU's"

(*) Remark :
Uploading language display templates is only needed for delegate units with WDU SW version 1.12 or older.
Uploading language display templates can also be done via TIS2500 and TIS5500 user SW

12. Web server

12.1. Setup

12.1.1. Summary

Device information

General device information is summarized in this section.

- *System Name:* Displays the system name. Configured in the TCP/IP settings page.
- *IP Address:* Displays the device IP address.
- *Subnet Mask:* Displays the currently configured IP subnet mask.
- *Address Mode:* Displays the protocol used to define the IP address.
- *Base MAC Address:* Displays the device MAC address.

System Information
Here you can find information about the components inside the system.
Hardware components and software components each have their own version.

- *Serial Number:* Displays the serial number of the device.
- *Model Name:* Displays the device model name.
- Hardware Version: Displays the hardware version number.
- *Boot Version:* Indicates the system boot version currently running on the device.
- *Firmware Version:* Displays the firmware/software version.
- *FPGA VHDL Version:* Displays the VHDL version for the FPGA.

- *RF hardware 1 Version:* Displays the RF hardware version for the active module.
- *RF hardware 2 Version:* Displays the RF hardware version for the passive module.
- *RF Firmware 1 Version:* Displays the RF firmware version for the active module.
- *RF Firmware 2 Version:* Displays the RF firmware version for the passive module.

Note:
Use this information when you contact the service department in case you experience problems with the system.

12.1.2. TCP/IP settings

Identification

- *System Name:* Defines the user-defined system name.
- *Base MAC Address:* Displays the MAC addresses assigned to the system.

IP configuration

In this section you can configure how the system will acquire its IP address

- *IP Address Mode:* Retrieves the IP address using DHCP or Static.

  DHCP: Retrieves the IP address using DHCP.
  Static: The IP address is statically defined.

- *IP Address:* Defines the system IP address.
- *Subnet Mask:* Defines the system IP address mask.

Note:

When pressing the 'Save' button, the active settings are stored in memory and recalled after power-down.

12.1.3. Country selection

Select the correct country the system is working in. This setting will affect the available frequencies and output power of the HF-carriers.

12.1.4. Admin

Change password

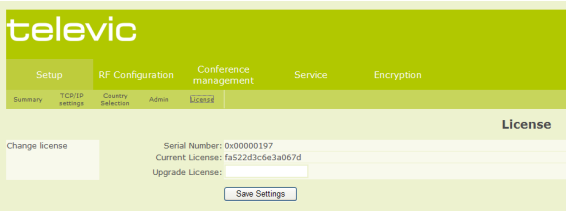
Only users that know the password are authenticated to use and consult the Confidea WCAP web pages!

In this section the password can be redefined:

1. Enter the OLD password
2. Enter a new password (Max. 50 characters long)
3. Confirm the new password
4. Submit the values to the server and wait for the result.

Note:
The old password will work as long as no positive feedback has been received.

12.1.5. License



The license can be upgraded to use max. 56 channels in stead of 16. Each license code is linked to the serial number of the WCAAP.

12.2. RF Configuration

12.2.1. General

Power

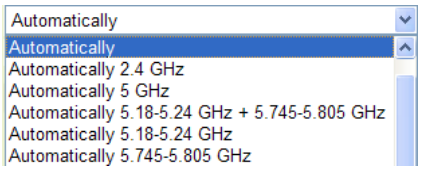
Room size: the transmitted output power will be adjusted to cover the configured room size.

The system will select the appropriate power setting when the auto setting has been selected

Frequency

The drop down list box allows you to select the frequency on which the system needs to operate.

Automatically



When the 'Automatically' setting has been selected, the system will decide automatically on which frequency to operate, based on its measurements of the available spectrum. In this way, interference with equipment that operates nearby is avoided.

From AP SW 0.11 onwards , there is the possibility to specify a preferred frequency range .

Frequencies listed in BLACK color.

When one of the frequencies is selected out of the list, the system will be forced to work on that frequency and will not automatically switch to another channel in the case that interference should occur.

Frequencies listed in BLUE color.

Some frequencies require a special procedure before equipment can occupy the channel. These frequencies are indicated with a blue color. Compliancy with the ETSI EN301893 standard requires a channel availability check on these special frequencies before one of these frequencies can be used.

This also implicates that, although an operating frequency has been manually selected, the system will still switch to another available channel when a radar signal or other interfering signal has been detected on that channel.

Note:
The channel availability check takes 60 seconds. During that time delegate units cannot connect to the Confidea Access Point

Frequencies listed in light BLUE color.

A channel where radar detection is necessary and the availability check has been performed.

Frequencies listed in RED color.

Some frequencies will be marked in red indicating that an interfering signal was detected on that channel. The interference severity can be monitored in the quality pages.

Frequencies listed in dark RED color.

In a channel where radar detection is necessary, an existing signal has been detected.

12.2.2. Quality 2.4 GHz ISM

Channel Quality

On this webpage the expected quality for each possible RF channel in the 2.4GHz ISM band can be monitored.

This visualization of channel availability and quality helps to select a fixed RF channel in case the system is set not to work in automatic mode.

See also notes on Page 54

Note:
The channel availability is visualized using colors:

- A full **GREEN** bar indicates the channel is available 100% of the time. This channel is thus safe to use.
- A full **RED** bar indicates the channel is fully occupied by other radio devices. This channel should not be used to operate the wireless Confidea system.
- The more activity on a channel, the more the corresponding bar will color RED, and thus the more likely interference will occur with other systems.

12.2.3. Quality 5.15 – 5.35 GHz

On this webpage the expected quality for each possible RF channel in the 5.15-5.35 GHz band can be monitored.

This visualization of channel availability and quality helps to select a fixed RF channel in case the system is set not to work in automatic mode.

12.2.4. Quality 5.47 – 5.725 GHz

On this webpage the expected quality for each possible RF channel in the 5.47-5.725 GHz band can be monitored.

This visualization of channel availability and quality helps to select a fixed RF channel in case the system is set not to work in automatic mode.

Note:
From time to time, the Confidea wireless system will also measure its own activity in the channel on which it is currently operating.
This results in a RED indication on the corresponding bar graph, but does not affect the reliable operation of the system.

12.2.5. Quality 5.8 GHz ISM

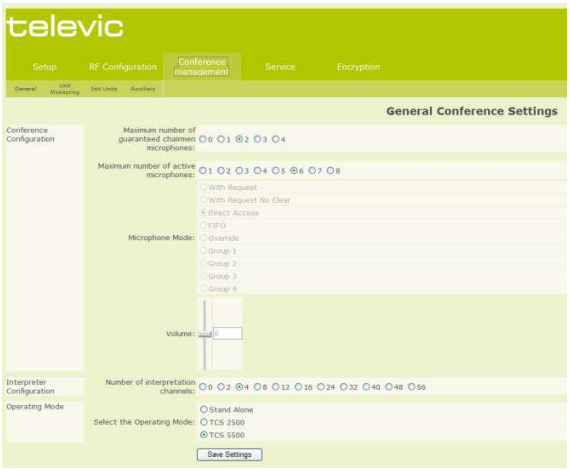
On this webpage the expected quality for each possible RF channel in the 5.8 GHz ISM band can be monitored.

This visualization of channel availability and quality helps to select a fixed RF channel in case the system is set not to work in automatic mode.

12.3. Conference Management

12.3.1. General

Conference Configuration



– *Maximum Number of Guaranteed Chairman Microphones:*

Defines the maximum number of chairmen microphones that can be activated on top of the already active microphones , even if the maximum number of active microphones is already reached. The system can handle a total number of max. 8 active microphones , including chairman microphones.

Remark:
Max 1 chairman can be used in stand-alone mode. The Confidea CS software or Confidea central unit can be used if more than 1 chairman units are required.

Note:
Choosing a high number of active microphones will limit the number of interpretation channels.

– *Maximum Number of Active Microphones:*
Defines the maximum number of simultaneous active microphones. The system can handle a maximum number of 8 active microphones.

– *Microphone Mode:*
Defines the conference mode.

With Request:

Enables the participant to send a request to speak to the chairman or conference operator by pressing the microphone button (or to cancel his request by pressing the microphone button again). Once the floor is requested, the green LED on the right side of the microphone button will flash. This means that the conference unit is in request mode.

The chairman or conference operator grants the participant the permission to speak by using the NEXT button or by clicking the green microphone on the computer screen in case the Confidea wireless system is connected to a central unit and PC control software is used.

While the conference unit is in request, the indicator ring of the microphone will flash.

With Request No Clear:

Enables the participant to send a request to speak to the conference operator or chairman. However, he cannot cancel his request. The chairman or conference operator grants the participant the right to speak by using the NEXT button or by clicking the green microphone on the computer screen in case the Confidea

wireless system is connected to a central unit and PC control software is used.

While the conference unit is in request, the red signal ring of the microphone will flash.

Direct Access:

Enables the participant to turn on or off his microphone at any time. The only limitation here is the maximum number of microphones that may be active simultaneously.

FIFO:

In this conference mode, only one microphone can be active at a time without intervention of the conference operator. Activation of another microphone switches off the current active microphone.

The only exception here is that the chairman microphone can always be activated..

Override:

Works like the FIFO mode; however multiple microphones can be active at the same time. The number of microphones that can be active simultaneously is set by "Maximum Number of active Microphones" setting.

When the maximum allowed number of microphones are switched on, activation of an additional microphone will automatically switch off the microphone that was active for the longest time. Again, the Chairmen units can always be activated, regardless of the number of microphones already switched on.

Group 1:

Enables one microphone at a time to be active without a request for activation. Other participants can switch their microphone in request mode; the first applicant gets the floor when the delegate who has the floor turns off his active microphone or when the chairman or conference operator grants the participant the permission to talk by using the NEXT button or by clicking the green microphone on the computer screen.

Group 2:

Enables two microphones to be active at the same time. Other participants can switch their microphone in request mode; the first applicant who requested the floor gets the floor when one of the currently active microphones is turned off or when the chairman or conference operator grants the participant the permission to talk.

Group 3:

Works the same way as Group 1 and Group 2, with the alteration that three participants can have the floor at the same time.

Group 4:

Works exactly like Group 1 and Group 2, with the alteration that four participants can have the floor at the same time.

Note:
The setting *Maximum Number of Active Microphones* has priority over the group setting , so regardless the chosen group setting , the number of participants that can have the floor at the same time is always limited by the *Maximum Number of Active Microphones* setting.

Note:
If the Confidea wireless system is connected to a Televic conference system central unit, the conference mode settings will be managed from that central unit.

Reference:
When using Confidea wireless in conjunction with other Televic conference systems and PC control software, please refer to the User Manual of those systems for more information on the use and setting of the various conference modes.

– *Volume:*
Defines the loudspeaker volume.

Interpreter Configuration

Defines the number of broadcasted interpretation channels. A (default) maximum of 16 interpreter channels can be set.

The amount of available channels can be upgraded by license to a max of 56 (see also chapter 12.1.5)

Note:
Choosing a high number of interpretation channels will limit the number of maximum microphone channels.

Note:
Although it is possible to select the highest setting of number of active microphones together with the highest number of interpretation channels, it is advised to use the settings that are not marked in red!

Using settings marked in red may influence audio quality and max. reach

Operating Mode

The selection between “stand alone” mode (without the use of a central unit) and Confidea CU or TCS5500 CPU can be made.

12.3.2. Unit Monitoring

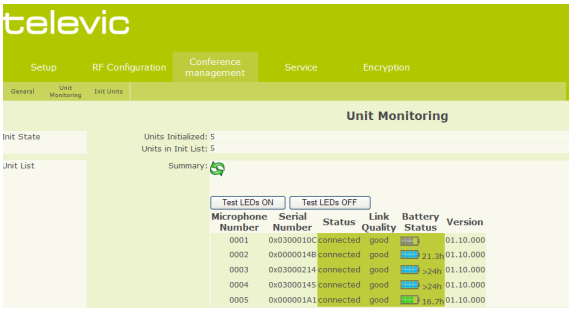


Figure 12: Unit monitoring List

Init State

- *Units Initialized:* Displays the number of initialized units currently linked to the system.
- *Units in Init List:* Displays the total number of initialized units in the list.

Unit List

In this section a unit summary is displayed.

- *Microphone Number:*
  Displays the microphone number.
- *Serial Number:*
  Displays the unit serial number.
- *Status:*
  Displays the unit status. Units can either be '**Connected** 'or '**Disconnected'**.
- *Link Quality:*

  Displays an indication of the quality of the radio link the unit and the Confidea access point. The quality is expressed as **Excellent**, **Good**, **Fair** and **Low**.
- *Battery status:*

  Displays the remaining battery capacity. The value indicates how many hours the unit can still be used before the rechargeable battery is depleted.
- *Version*

  Displays the SW version of the delegate units

Note:
The information on the unit monitoring page is not refreshed automatically.
To view the most recent condition of the system, click the "**Refresh Unit Table**" button.

Note:
During the first minutes a unit is switched on, the battery status is not accurate and higher values can be displayed. This is caused by an averaging process and notby the behavior of the batteries.

12.3.3. Init Units

Init State

- *Units Initialized:*
  Displays the number of initialized units currently linked to the system.
- *Units in Init List:*
  Displays the total number of initialized units included in the list

Init

Init Control:

- *Open Access:*
  When the system is set to 'Open Access' any delegate or chairman unit that powers up within the range of a Confidea Access Point will log itself on to that access point, and its ID will be added to the Init List
- *Manual:*
  In manual mode, each units needs to be initialized manually, by pressing the microphone button, before it is added to the Init List.

- *'Start Init':*
  Pressing this control will start an initialization cycle. The green and red Microphone Status LEDs wil blink until the delegate unit has been recognized as ready to log on, by the Confidea Access Point. Once recognized , only the red Microphone Status LEDs will blink . Now the units are ready to initialize. Pressing the microphone button of each unit that needs to log on to the system , will register that unit within the Access Point.
- '*Save and Stop Init'*:
  This will stop the initialization and save the init list to memory. To add more units, restart the init cycle.
- '*Clear Init List*:
  This will clear the init list and allow you to start from scratch to build an init list.
  To add delegate units to an existing initialization, just start init without clearing Init list.

12.4. Service

12.4.1. Logging

Log List

On this web page, a list of events are displayed that occurred in the access point. This will help to diagnose the system when necessary.

- *Start:*
  This button starts capturing the access point events.
- *Stop:*
  This button stops capturing the access point events.
- *Clear:*
  This button will clear the events that were previously captured.

Use the MS Windows Copy-Paste facilities to export the log list.

12.5. Encryption

12.5.1. Key Assignment

Introduction

To ensure a highly secured wireless system, the Confidea wireless system uses an encryption algorithm and mechanism that is fixed and cannot be changed.

The information that is transmitted over the radio link is encrypted with a key to make it inaccessible for 3rd party equipment. This key is default and identical for all Televic units.

Security can be increased by adding a custom key, that is specific to a certain set-up or installation. Only the units and access point that share the same encryption key are able to communicate with each other. In this way, the system has become customer

exclusive and as a result an even higher degree of security has been reached. One default key and 15 custom keys can be used.

(see also chapter 14 Encryption)

Encryption Key

- *Default Key:*
  When selecting this key, information over the wireless link is encrypted, using the Televic default key, used by all Televic equipment
- *Custom Key:*
  To further increase security, or to limit the access to the Access Point only to a well controlled number of delegate units, a custom key can be generated and sent to those units that are allowed to join. The result of this action is that only the units that know this key can access the system and participate in the conference
- *'Calc.l'* key:
  Pressing this button will randomly generate a 128 bit key. The key appears in the window and can still be edited by the user.
- *'Upload'* key:
  Pressing this button will upload the custom key to all units, currently logged on to the system. Units can only obtain the customer specific key during initialization. As soon as the initialization has been closed it will not be possible to access the system with other units.

13. Initialization

13.1. Introduction

The system can be controlled by the *WCAP* in stand-alone mode or together with the Confidea CU / TCS5500 Central unit in coupled mode.

In stand-alone mode it is not required to initialize the units. However, if you want to authorize the wireless units that will be connected into the system you can follow the unit initialization procedure.

In coupled mode, the same initialization procedures have to be followed as defined in the documentation from the central unit.

To personalize the system and to further extend the confidentiality of your wireless conference system a unique encryption key can be defined.

13.2. Stand-alone mode

13.2.1. Access modes

When you use the Confidea wireless system in stand-alone mode, i.e. with no connection to a Confidea CU or TCS5500 central unit, the *WCAP* is responsible for the unit initialization and access control.

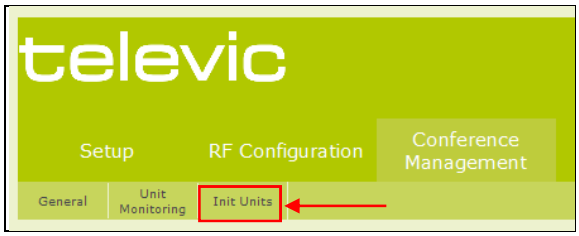
In stand-alone mode, the *WCAP* supports two kinds of access: **open access** and **controlled access**.

- **Open access:** This is the default mode. Any unit can connect to the WCAP without authorization procedure
- **Controlled access**: a unit can only connect after going through an initialization and authorization procedure.

13.2.2. Selecting the Access Mode

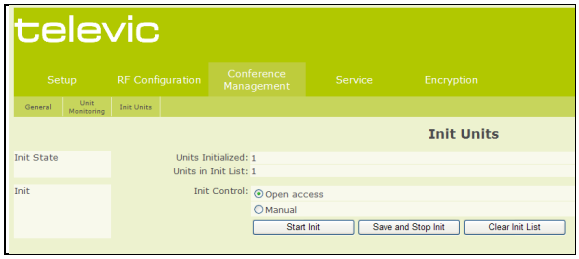
To select the desired access mode go to the “Init Units” sub tab in the “Conference Management” menu from the web server (refer to Figure 13.1)

Figure 13.1: Web server init page selection



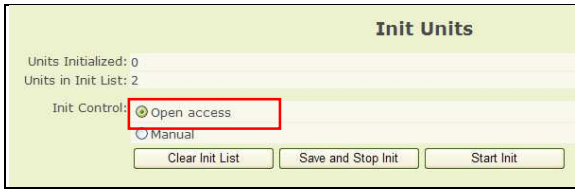
The following screen will appear:

Figure 13.2: Unit init page



To select 'Open Access' click the radio button next to 'Open Access' on the 'Init Units' page (refer to Figure 13.3)

Figure 13.3: Init units page - Open access



Select this mode if the wireless units are not required to be authorized, before they are allowed to connect with the *WCAP*.

This mode is especially useful for a fast setup.

Note:
Avoid using **Open Access** in areas with more than one active Confidea wireless system, as there is no control over which *WCAP* the delegate units will connect to.

To select 'Controlled Access' click the radio button next to 'Manual' on the 'Init Units' page (refer to Figure 13.4)

To control which wireless units connect with the *WCAP* a manual initialization of the units is required.

Figure 13.4: Init units page - Manual

13.2.3. Unit initialization in 'Open Access' mode

Switch on all wireless units and wait a few seconds until the units have discovered the WCAP (see chapter 10)

All active wireless units will automatically connect with the *WCAP* and join the conference.

13.2.4. Unit initialization in 'Controlled Access' mode

In this mode, a manual initialization is required.

The manual initialization procedure requires the use of the 3 buttons on the web server displayed above: "Start Init", "Save and Stop Init" and "Clear Init List".

Take the following steps to initialize all units:

1. Switch on all wireless units and wait a few seconds until the units have discovered the WCAP
2. Select the "Clear Init List", Clear Init List, to clear any previously created initialization list.
3. Start the new initialization by selecting the "Start Init", Start Init ,button.
   After you started the new initialization, the red Microphone Status LED's on all wireless units will start to blink.
4. To add a unit to the initialization list, press the microphone button of the unit to add.

5. The LEDs will go out indicating that the unit has been added to the list.
6. Repeat step 3 for each unit that needs to be added.
7. When finished, stop and save the initialization by pressing the "Save and Stop Init" button, Save and Stop Init .

Only the units that have been initialized and listed in the Init List will now be able to join the conference.

The init list is stored in the *WCAP* and stays in memory even after switching the *WCAP* off.

Next time the *WCAP* and delegate units are switched on, only these units that are in the Init List will be allowed to connect to the *WCAP*.

13.2.5. Adding a new unit in 'Open Access' mode

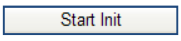
In '**Open access**' mode, adding a unit requires simply to switch the unit on.

It will then automatically connect to the *WCAP* in operation.

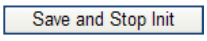
Note:
When multiple *WCAP*s with 'Open Access' are in operation in the same area, there is no control over which *WCAP* the new unit will connect to.

13.2.6. Adding a new unit in 'Controlled Access' mode

In a '**Controlled Access**' set-up, adding a unit requires the following steps:

1. Switch on the wireless unit to add and wait a few seconds until the unit has discovered the WCAP
2. Open the existing initialization by selecting the "Start Init", 

, button.
3. After you started the new initialization, the red Microphone status LED's on the wireless unit(s) will start to blink. The LED's on the units that are already known in the init list will automatically go out.
4. Add the new wireless unit(s) by pressing the microphone button on the unit(s).

5. Stop and save the initialization by pressing the "Save and Stop Init" button, 

.

13.2.7. Reviewing Init information

At any time it is possible to see how many units are known by the system, “Units in Init List”, and to see which units are actually connected with the *WCAP*, “Units Initialized”.

This information is visible in the “Unit Monitoring” and “Init Units” sub tabs in the “Conference Management” menu (see Figure 13.2)

Figure 13.5 shows the information on the screen when 1 unit is listed in the Init List but not connected with the *WCAP*:

Figure 13.5: Init example 1

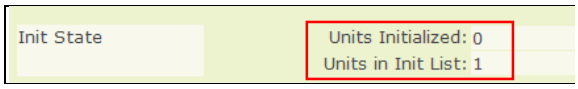
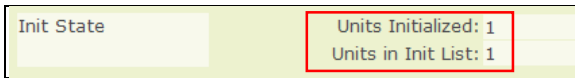


Figure 13.6 shows the information on the screen when 1 unit is listed in the Init List and this unit is switched on and connected with the *WCAP*:

Figure 13.6: Init example 2



13.3. Coupled mode

If the *WCAP* is used in combination with a wired central conference unit, e.g. Confidea CU or TCS5500, then the initialization procedure explained for that wired unit has to be followed.

Note:
The Init control like displayed in the web server has no functionality when the *WCAP* is coupled with another wired conference unit.

Reference:
Refer to the manual of the connected central unit for the initialization procedure

14. Using Encryption

14.1. Introduction

To secure all communication between the WCAP and the wireless delegate units, all information that is passed over the radio link is encrypted by default, using a default encryption key. This key is identical for all Confidea wireless equipment.

To this default key, a custom encryption key can be added. This further enhances the confidentiality, but can also be used to control access in an environment where multiple adjacent rooms are using a Confidea wireless conference system. In this way, access can be restricted to a single room or a selection of rooms. The custom key as it were adds a unique relationship between a wireless unit and a given access point.

14.2. Default encryption

By default the system uses an encryption mechanism that is known by each unit in the wireless conference configuration.

By using this setting it is possible to add new units in the conference configuration or using the delegate units with other *WCAP*'s at any time

Note:
The advanced encryption mechanism used in the Confidea wireless system makes decryption by third party equipment practically impossible.

14.3. Setting the default encryption

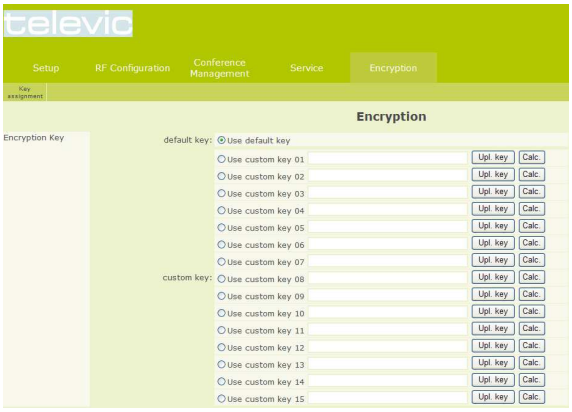
The default encryption mechanism can be set by following these steps:

1. Select the "Key assignment" sub tab in the "Encryption" menu from the web server.

Figure 14.1: Web server key assignment page selection

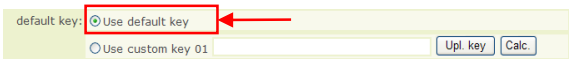
The following screen will appear:

Figure 14.2: Key assignment page



2. Select the "Use default key" option to return to the default encryption mechanism

Figure 14.3: Default key selection



14.4. Custom encryption

The Confidea wireless conference system can be personalized by defining and selecting a unique encryption key.

Note:
The basis of the encryption mechanism cannot be altered, so adding a custom key does not affect the encryption strength.
Default- and custom encryption yield an encryption strength that is equally high.

By using a customized key, only the units that have this key, i.e. on which the specific key has been uploaded, can connect with the *WCAP*. All other units will be rejected.

It is impossible to receive the transmitted audio signal with a unit that does not have the customized key.

Up to 15 customized encryption keys can be defined.

Note:
Once uploaded to the delegate units, custom keys cannot be retrieved from the system.

14.5. Setting a customized encryption

To set up your system with a custom encryption key, carefully follow these steps:

Step 1 - Check your configuration

Before uploading the custom key check if all units in your system are switched on and connected to the *WCAP*. Verify if the correct number of units is logged-on by checking the "Units Initialized" number which can be found under the "Unit monitoring" or "Init Units" sub tabs in the "Conference management" menu. Please refer to the initialization chapter (ref.) for more information.

Note:
If delegate units have received custom keys in the past, it may be necessary to select the default encryption mechanism first, (refer to chapter 14.3 Setting the default encryption) to allow each unit in the system to access the WCAP.

Step 2 – Go to the Key assignment web page

Select the "Key assignment" sub tab in the "Encryption" menu from the web server (refer to Figure 14.1.)

The key assignment page will appear (refer to Figure 14.2)

Step 3 – Enter a new encryption key

In this example we will modify custom key 1.

To manually enter a new custom key, choose a 32-character long encryption key and manually enter it in the text box next to the "custom key 1" mark (refer to Figure 14.4).

Caution:

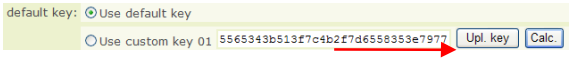
Only use hexadecimal characters i.e. choose 32 characters from the following list:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f.

If a key shorter than 32 characters has been entered, then the remaining positions will be filled with zeros.

If a key longer than 32 characters has been entered, then the key will be truncated after the first 32 characters.

Alternatively, the system can generate a random 128-bit (32 hex characters) encryption key for you. To do this, click the "Calculate 128-bit full key" button (refer to Figure 14.4).

Figure 14.4: Custom key entry field



Step 4 – Upload a new encryption key

After a key has been generated it must be uploaded into the system. Not only the *WCAP*, but also all wireless delegate units that need to connect with the *WCAP* must know the same key.

Upload the key by clicking the "Upload key" (refer to Figure 14.4)

Note:
During the upload, the microphone LEDs will flash.
Once the upload is successful, the LEDs go out.

Caution:

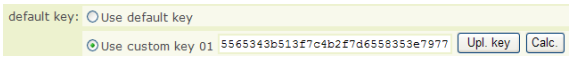
Only the units that are connected with the WCAP can receive the newly generated encryption key.

Other units will be ignored!

Step 5 – Activating the new encryption key

The *WCAP* will start encrypting the transmitted data and audio after a custom key has been selected.

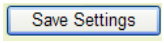
Figure 14.5: Custom key selection



Caution:

Wireless units not containing the same encryption key as selected, because they were not connected with the WCAP at the time of upload, can no longer connect with the same WCAP.

The units will be ignored by the system!

If the *WCAP* needs to use the selected key next time it powers up, push the 

button.

14.6. Adding a unit with a customized encryption

Follow the next steps to add a new unit in a Confidea wireless system that is configured to use a customized encryption key.

Step 1 – Select the Default encryption key

Please refer to the Setting the default encryption (ref.) for more information.

Step 2 – Initialize the new unit

Add the new unit to the initialization list. This step is only required if the access point is configured to work in manual initialization mode. Otherwise the unit will be automatically initialized. Please refer to the initialization chapter (ref.) for more information.

Step 3 – Apply the customized encryption key to the initialized units

After the new unit is initialized the customized encryption key can be assigned to the newly added units. Therefore follow the steps described in the Setting a customized encryption section (ref.).

14.7. Using multiple customized keys

It is possible to assign up to 15 different encryption keys. You can update all your units with the customized keys or just a subset. This way you can select the units that can join the conference by selecting the appropriate encryption key.

15. Auxiliary in/out

15.1. Introduction

On Confidea Access Point Plus (WCAP+) , auxiliary balanced analog input and output are available. So for basic systems , no additional central equipment is needed to connect the system to an external public address system or to add an external signal to the conference system.

Additionally it is possible to connect the access point to a video conferencing system using the distance conferencing setting

Fig 15.1 : Aux balanced input – output

15.2. Use of Auxiliary input - output

For both auxiliary input and output , status can be set to on or off and volume can be adjusted.
When WCAP+ is used in Stand Alone mode , there are also “N-1” and “External processing” options available .

15.2.1. Distance conferencing

Distance conferencing (= N-1) option adds external signal , via aux in , to the local floor signal and sends the local floor signal , via aux out , to the remote party.

15.2.2. External Processing

Activating the “external processing” option allows to add external signal processing equipment or a mixing board.

15.3. Selecting auxiliary input/output settings

When a WCAP+ is used , “conference management” menu contains an additional “auxiliary” sub tab as shown below.

The distance conferencing and external processing options are only available in stand alone mode , and are disabled in coupled mode . In coupled mode , distance conferencing and external processing remain possible via Confidea CU or CPU5500.

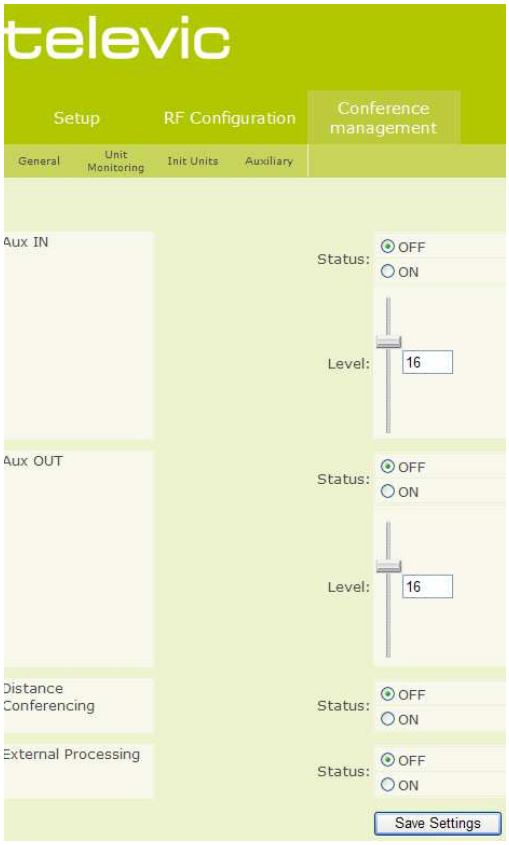


Fig 15.3.1 : Aux balanced input – output

15.4. Signal paths

15.4.1. Stand alone mode

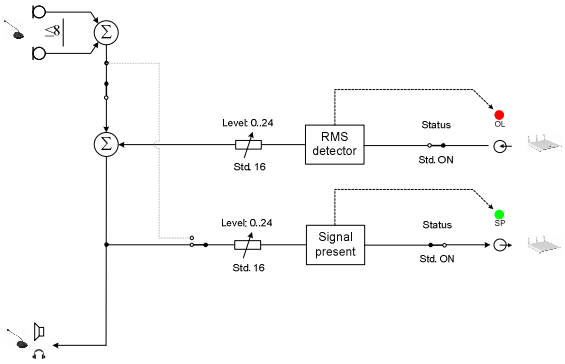


Fig 15.4.1 signal path stand alone

15.4.2. External processing

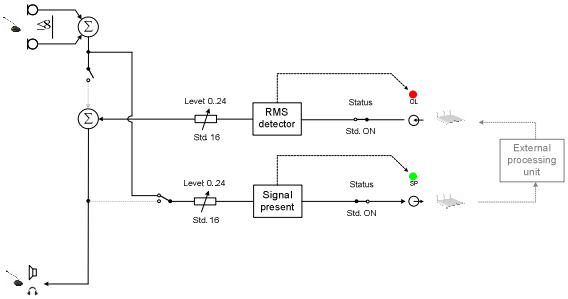


Fig 15.4.2 signal path external processing

15.4.3. N-1 or Distance Conferencing

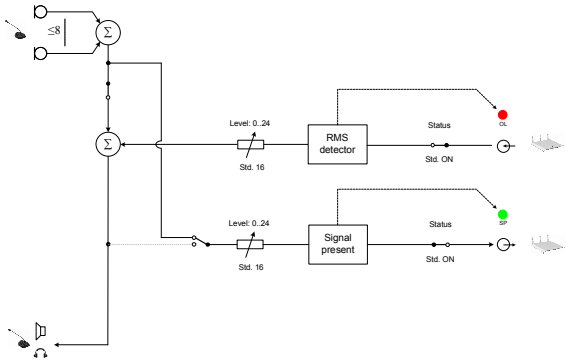


Fig 15.4.3 signal path N-1

15.5. Aux signal levels

Level IN/OUT	Gain (dB)
--24-	+24
- 23	+21
22	+18
21	+15
20	+12
19	+9
18	+6
17	+3
16	0
15	-3
14	-6
13	-9
12	-12
11	-15
10	-18
09	-21
08	-24
07	-27
06	-30
05	-33
04	-36
03	-39
02	-42
01	-45
00	OFF

Fig 15.5.1 Aux levels

Section 4 – Use Cases

16. Stand alone system

16.1. Basic discussion

In a basic setup where only discussion is applicable, the Wireless Conference Access Point WCAP (see link to chapter WCAP) acts as a central control unit.

This means the system can operate without the need of an extra central control unit (Confidea CU or CPU5500).

Units applicable to this setup are listed below:

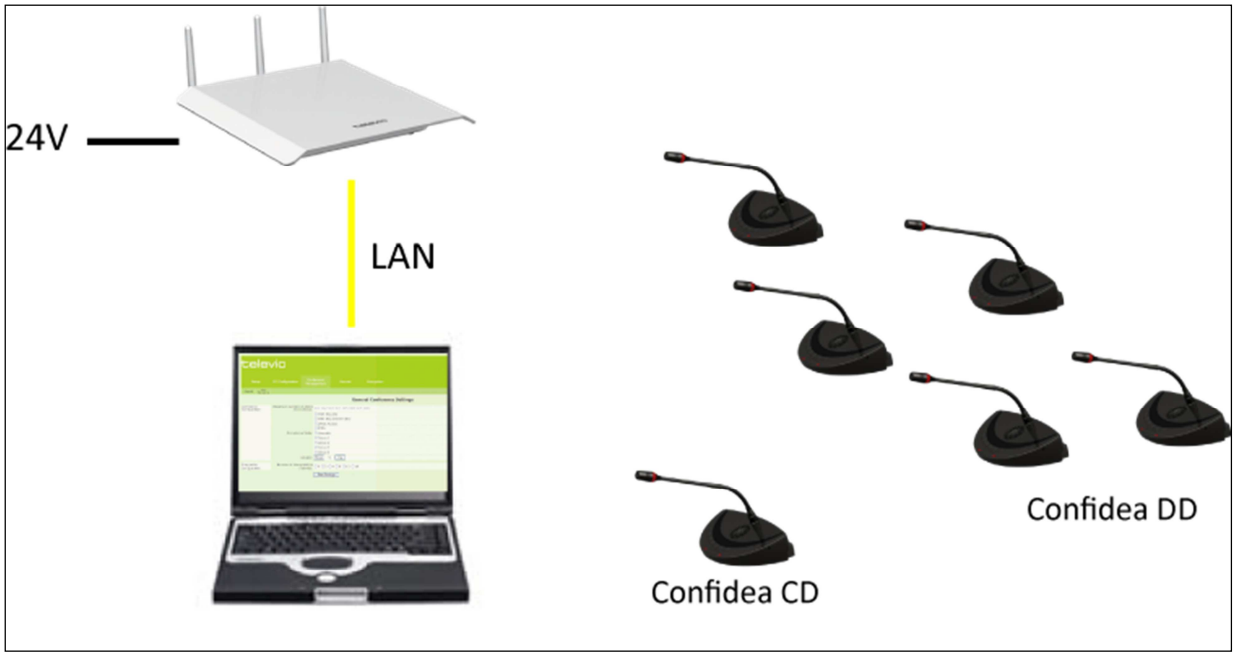
- Confidea DD
- Confidea CD

In a standalone configuration power needs to be supplied to the WCAP separately. (see chapter WCAP power supply)

Configuration and monitoring of the system can be done via the build-in web server, which is accessible via a standard web browser. (See section 3 system configuration)

Note:
In this case the chairman needs to guide the meeting by using his prior and nextbutton. Microphone activation by an operator is not possible via web server application.

Figure 16.1: Stand alone set up for basic discussion



16.2. Basic voting and opinion polling

In a setup where there is only a need for basic voting or opinion check, the Wireless Conference Access Point WCAP (see link to chapter WCAP) acts as a central control unit.

This means the system can operate without the need of an extra central control unit (Confidea CU or CPU5500).

Units applicable to this setup are listed below:

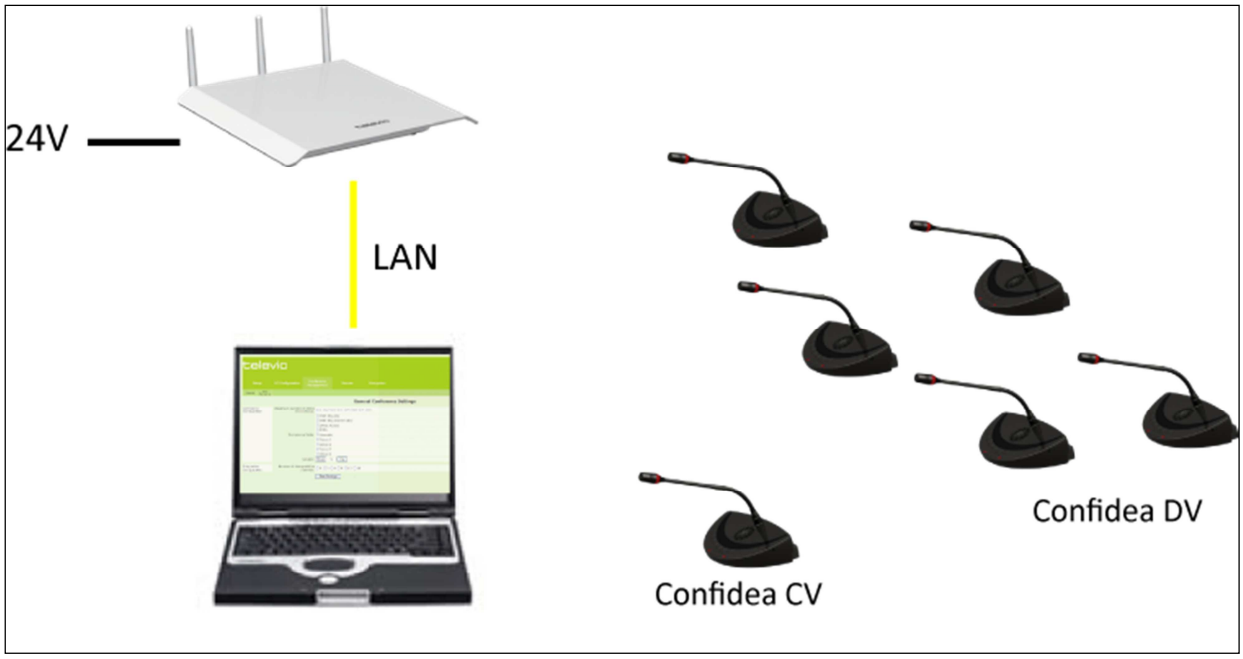
- Confidea DV (**Figure 6.1** and **Figure 6.**)
- Confidea CV

In a standalone configuration power needs to be supplied to the WCAP separately. (see chapter WCAP power supply)

Configuration and monitoring of the system can be done via the build-in web server, which is accessible via a standard web browser. (See section 4 system configuration)

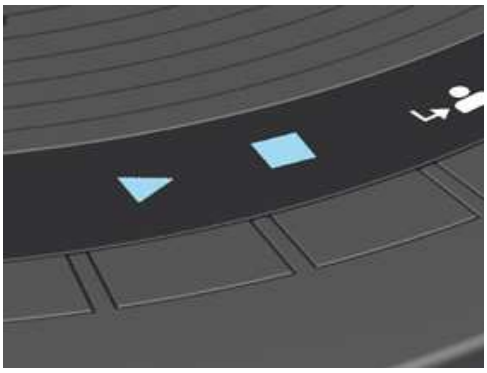
Note:
In this case the chairman needs to guide the meeting by using his prior and next-inline button. Microphone activation by an operator is not possible via web server application.

Figure 16.2: Stand alone set up for opinion polling



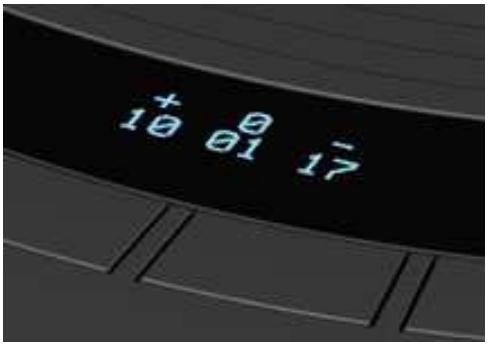
Chairman has control over the voting session. With the voting session control buttons (see Confidea Wireless units - Controls and indicators) he can start, pause or stop a voting session.

Figure 16.3: Voting control buttons



After pressing the stop button, the voting session is terminated and the results are distributed to the information display of all registered Confidea WDUs.

Figure 16.4: Voting information display



Pressing the stop button a second time clears the voting results.

Note:
The voting results are not stored in a file in this setup. In case there is a need see use case CE2500 or CPU5500

17. Connected to CE2500, Confidea CU or CPU5500

As the Confidea wireless system is an addition to the Televic product family it is also possible to combine the Confidea wireless system with the existing /Confidea CU and TCS5500 system (refer to

Figure 17.3: Televic Family concept)

This family approach makes it possible to create a conference system fitting every customer needs.

In situations where every now and then an extension of the fixed conference system is required, adding some wireless units can reduce the setup costs drastically.

Depending on the demands of a project the central control equipment of the TCS2500 , Confidea CU or TCS5500 does the job.

The Confidea access point (WCAP) can be directly connected to one of the digital output busses of the TCS2500 central control unit or Confidea CU

Figure 17.2 WCAP connected to Confidea CU

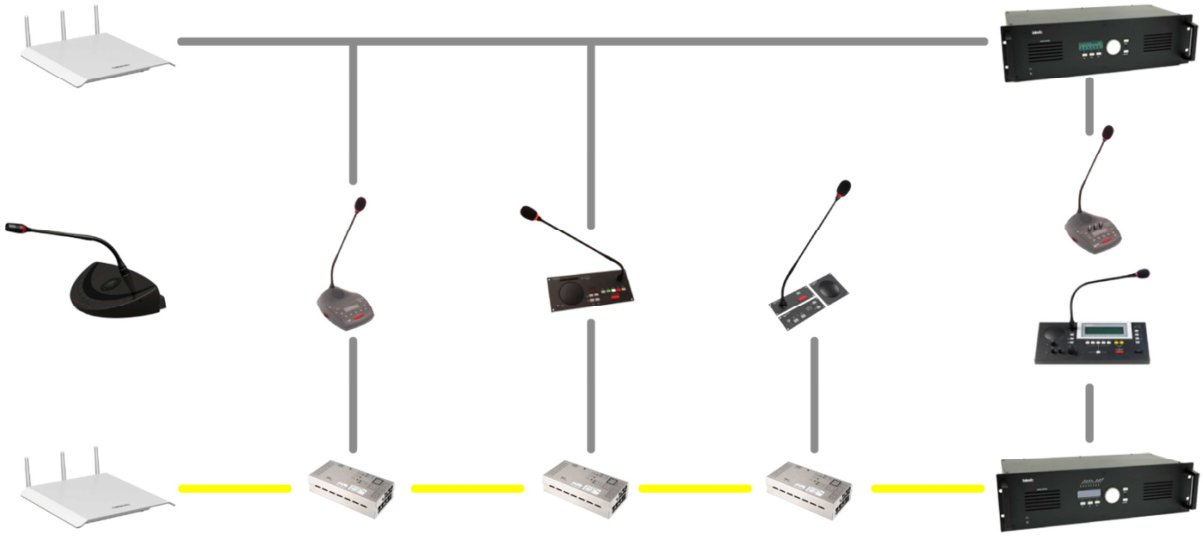
Connecting the Confidea access point to the central control equipment of the TCS5500 requires an additional splitter unit (SPL5525); Confidea Access Point is then connected to one of the “P…” ports of the splitter.

Figure 17.1WCAP connected to CPU5500

In the following section three possible applications are described. This will help to define the correct system architecture for a given project.

Reference:
When using Confidea wireless in conjunction with other Televic conference systems and PC control software, please refer to the User Manual of those systems for more information.

Figure 17.3: Televic Family concept

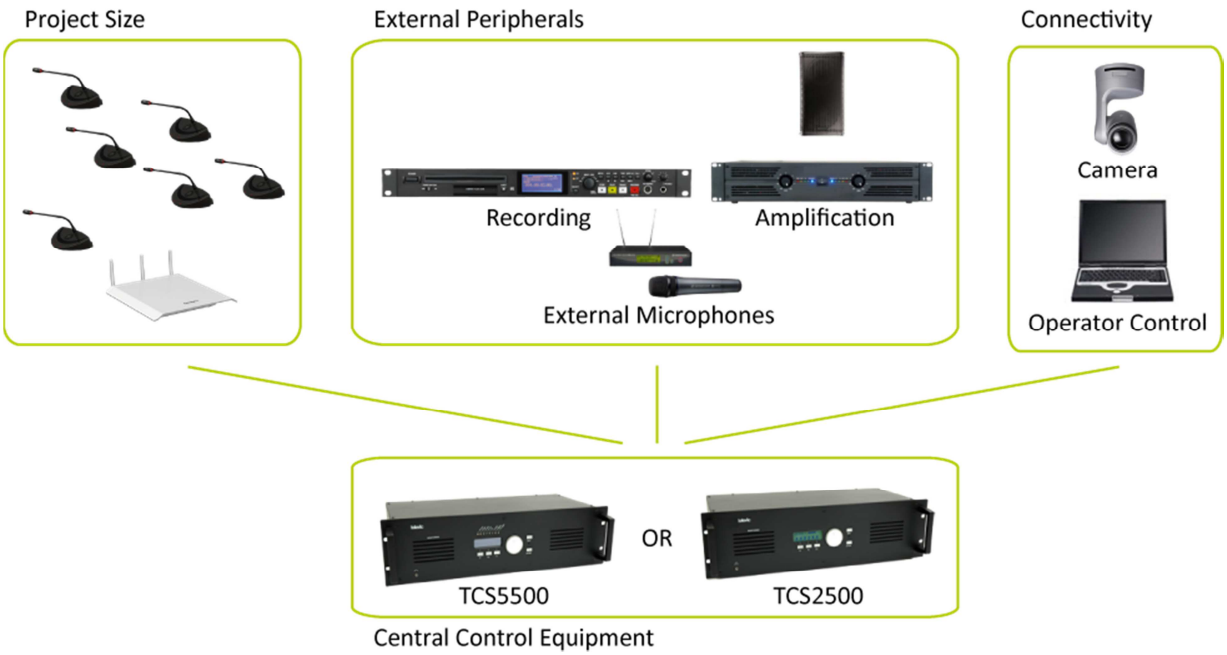


17.1. Discussion

For these applications, delegates of the meeting have a contribution unit with only a microphone to participate in an ongoing discussion.

Several criteria can influence the choice of the Televic central control unit to be used. The criteria described below should guide you in designing the best possible system architecture for a given project.

Figure 17.4: Central control equipment selection criteria



Project size

The number of participant units in a meeting will influence the decision on the system to use.

The TCS2500/ Confidea CU central control unit is limited up to 120 active wired delegate units.

Projects requiring a larger number of participants should use the TCS5500 central control unit with expandable system architecture.

Table 17.1 below gives an overview on the system compatibility.

Table 17.1: Project size vs. Televic system

Number of Participants	TS2500 or Confidea CU	TCS5500
< 50 wired	• (CE2500/B)	•
max 120 wired + wireless	• (CE2500 upgrade full option Or Confidea CU)	•
> 120 wired + wireless	–	•

External Audio Peripherals

PA systems:

Whereas the Confidea WDUs have a build in loudspeaker, some meeting rooms are equipped with external PA systems with loudspeakers installed on walls or in ceilings.

Making use of such a setup, the floor language of the conference system needs to insert into the PA system. This requires an analog output, which is available on the central control equipment of both TCS2500/Confidea CU and TCS5500.

Recording:

Whenever meeting reports need to be written or audio of meetings is being published on the web, recording needs to take place during the meeting.

The recording device (hardware or software solution) needs to have an analog input signal provided by the conference system. Both the Televic Confidua CU and the TCS5500 central control units have 7 analog outputs available. Additional outputs can be provided by adding external TCS5500 output equipment to the TCS5500 system.

Audio reproduction:

Feeding external audio signals (music before meeting, DVD sound, input external microphone, telephone line, …) into the conference system requires analog inputs on the central control unit. Both the TCS2500/Confidea CU and TCS5500 central control units have two analog inputs. If this is not sufficient the TCS5500 system has the capability to connect additional input equipment.

Table 17.2: I/O Equipment vs. Televic system

I/O	TCS2500/Confidea CU	TCS5500
Input	2	2 Expandable
Output	7 Expandable	7 Expandable

Connectivity

Operator Control:

Systems requiring a great degree of control can be equipped with the Televic software suite.

This application makes it possible, depending on the license, to control the microphones in a meeting, assign delegate names, control speech time, display delegate and speech time information on monitors or projection screens.

It offers easy initialization and configuration capabilities supporting an easy set-up and break-down, essential for successive meeting planning with low delays like convention centers.

Furthermore it visualizes the battery and RF quality status of all units, giving the operator/technician the ability to assure no interruptions once the meeting started.

Camera Control

To enable a camera system to visualize the currently active Confidea user, a device bus controller needs to translate the commands received from the Televic system into preset positions of the camera control system. Both the TCS2500/Confidea CU and TCS5500 systems will do the job.

The difference between the TCS2500/Confidea CU and the TCS5500 system on connectivity level is the way the communication takes place.

The TCS2500/Confidea CU uses a serial communication protocol, whereas the TCS5500 system has additional IP connectivity.
(Refer to Table 17.3: Connectivity vs. Televic System)

Table 17.3: Connectivity vs. Televic System

Connectivity	TCS2500/Confidea CU	TCS5500
RS232	●	●
TCP/IP	–	●

17.2. Advanced Voting

The stand alone voting setup can be seen as an informal voting session.

Making use of a Televic voting software suite enables following features:

- Voting agenda
- Voting session configuration options
- Voting result reporting
- Voting logging
- Voting result visualization

All of these options are available for as well TCS2500/Confidea CU as TCS5500 systems.

Main differences between the two systems are:

- Voting by authority
- Customizable voting result visualization

Table 17.4: Voting vs. Televic system

Voting	TCS2500/Confidea CU	TCS5500
Authority	–	•
Result visualization	fixed	customizable

17.3. Interpretation

Systems with simultaneous interpretation as a requirement always require a central control unit in combination with the interpreter desks.

Installation

Whereas the TCS2500 interpreter desks are of the table-top type, the TCS 5500 interpreter equipment can be semi-flush mounted.

Conformity Standard

The ID5500 interpreter desk is conform to the ISO 2603 standard and approved by interpreter organizations as the European Commission (SCIC), United Nation, AIIC.

Interpretation capabilities

The Confidea wireless system has the standard capability to send up to 16 languages to the contribution units. Both the TCS2500/Confidea CU and TCS5500 systems are capable of handling that number of languages.

An extra license is available to increase amount of languages to 40 when used in combination with TCS5500 . (see also chapter 12.1.5 : License)

External Equipment

As already described in External Audio Peripherals the number of analog outputs required for recording or needed to connect to an Infra red distribution system will determine the central equipment to be used.

Table 17.5: Interpretation vs. Televic system

Interpretation	TCS2500/Confidea CU	TCS5500
Installation	Table-top	Semi-flush mounted
Standard	xxxx	xxxx
# languages	Confidea : 16	Confidea : 16

Next to these points it is also possible to connect interpreter systems of other vendors. That way it is possible to use the Confidea wireless system without the need to change all the interpreter desks. The PIO unit of the TCS5500 plays an imported role in such configuration handling the floor and interpretation languages between the two systems.

+

Section 5 – Appendix

18. Default Settings

18.1. TCP/IP settings

18.1.1. Identification

- System Same: ***Confidea WCAP***

18.1.2. IP Configuration

- IP Address Mode: ***Static***
- IP Address: ***192.168.000.010***
- Subnet Mask: ***255.255.255.000***

18.2. Country Selection

- Country Selection: ***US/CA***

18.3. Admin

- Default password: ***123***

18.4. RF Configuration

18.4.1. Power

- Room Size: ***Big***

18.4.2. Frequency

- Frequency Selection: ***Automatic***

18.5. Conference Management

18.5.1. Conference Configuration

- Maximum number of active microphones: ***4***
- Microphone Mode: ***Direct Access***
- Volume: ***6***

18.5.2. Interpreter Configuration

- Number of interpretation channels: ***0***

18.5.3. Operating Mode

- Operating Mode: ***Stand Alone***

18.6. Init Control

- Init Control: ***Open Access***

18.7. Encryption

- Encryption mode: ***default encryption***